Chuyển giao dữ liệu cá nhân xuyên biên giới: Thực trạng pháp luật và một số giải pháp hoàn thiện

17/06/2026

TS. TRẦN NGỌC HIỆP

Khoa Pháp luật Dân sự – Trường Đại học Luật Hà Nội.

Tóm tắt: Bài viết phân tích thực trạng pháp luật Việt Nam về chuyển giao dữ liệu cá nhân xuyên biên giới. Qua đó, bài viết chỉ ra những điểm hạn chế về phạm vi áp dụng, điều kiện chuyển giao và các ngoại lệ không phải đánh giá tác động chuyển giao dữ liệu xuyên biên giới. Trên cơ sở tham chiếu kinh nghiệm quốc tế, bài viết đề xuất một số giải pháp nhằm hoàn thiện khung pháp luật, bao gồm việc ghi nhận bổ sung cơ chế về điều khoản hợp đồng mẫu và bổ sung yêu cầu đánh giá pháp luật của quốc gia tiếp nhận dữ liệu, hướng tới xây dựng cơ chế quản lý hiệu quả, phù hợp với chuẩn mực quốc tế, góp phần thúc đẩy phát triển bền vững nền kinh tế số Việt Nam.
Từ khóa: Dữ liệu cá nhân; chuyển giao xuyên biên giới; bảo vệ dữ liệu.
Abstract: This article analyzes the current state of Vietnamese law regarding cross-border transfer of personal data. It highlights limitations in terms of scope of application, transfer conditions, and exceptions to cross-border data transfer impact assessments. Drawing on international experience, the article proposes several solutions to improve the legal framework, including the introduction of standard contractual clauses and the requirement to assess the legal system of the recipient country, with the aim to establish an effective management mechanism aligned with international standards, thereby contributing to the sustainable development of Vietnam's digital economy.
Keywords: Personal data; cross-border transfer; data protection.

1. Tổng quan hệ thống pháp luật Việt Nam về chuyển giao dữ liệu cá nhân xuyên biên giới

Khung pháp luật hiện hành của Việt Nam điều chỉnh hoạt động chuyển giao dữ liệu cá nhân xuyên biên giới chủ yếu dựa trên năm văn bản pháp lý quan trọng: Luật An ninh mạng năm 2018, Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025, 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 (Nghị định số 356/2025/NĐ-CP), Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu (Nghị định số 165/2025/NĐ-CP). Trong số đó, Luật An ninh mạng năm 2018 đã đặt nền móng pháp lý đầu tiên cho vấn đề quản trị dữ liệu, với trọng tâm là bảo đảm an ninh quốc gia và xử lý các hành vi vi phạm trên không gian mạng. Cụ thể, khoản 3 Điều 26 của Luật này đã giới thiệu cách tiếp cận đầu tiên của Việt Nam đối với việc điều chỉnh chuyển giao dữ liệu xuyên biên giới thông qua yêu cầu nội địa hóa dữ liệu. Cụ thể, các doanh nghiệp cung cấp dịch vụ viễn thông, Internet

hoặc dịch vụ trực tuyến tại Việt Nam, nếu thu thập, phân tích hay xử lý dữ liệu liên quan đến cá nhân hoặc mối quan hệ của người dùng trong nước, thì bắt buộc phải lưu trữ dữ liệu đó tại Việt Nam trong một khoảng thời gian do Chính phủ quy định. Điều luật này phản ánh chính sách ưu tiên kiểm soát dữ liệu của Việt Nam, nhấn mạnh đến việc giám sát và phòng ngừa các mối đe dọa từ bên ngoài, đồng thời gắn vấn đề bảo vệ dữ liệu với yêu cầu bảo đảm an ninh quốc gia. Tuy nhiên, điểm đáng chú ý là Luật An ninh mạng năm 2018 không đặt ra lệnh cấm tuyệt đối đối với hoạt động chuyển dữ liệu ra nước ngoài, mà chỉ yêu cầu lưu trữ dữ liệu trong nước đối với một số trường hợp cụ thể. Tuy nhiên, tại thời điểm ban hành, Luật chưa thiết lập cơ chế hướng dẫn chi tiết để quản lý hoạt động chuyển giao dữ liệu xuyên biên giới, dẫn đến nhiều khó khăn trong thực tiễn tuân thủ đối với các doanh nghiệp.

Những hạn chế này ban đầu đã phần nào được khắc phục bởi Nghị định số 13/2023/NĐ-CP ngày 17/04/2023 của Chính phủ về bảo vệ dữ liệu cá nhân. Nghị định này đánh dấu bước ngoặt trong quá trình hình thành khung pháp luật bảo vệ dữ liệu của Việt Nam khi đưa ra các quy định chi tiết về bảo vệ dữ liệu cá nhân, đặc biệt tại Điều 25 quy định thủ tục chuyển dữ liệu cá nhân ra nước ngoài. Tuy nhiên, với tư cách là văn bản dưới luật, Nghị định số 13/2023/NĐ-CP vẫn bộc lộ một số hạn chế cả về phạm vi thẩm quyền lẫn nội dung, khiến việc thực thi trong thực tiễn chưa thật sự hiệu quả. Để tiếp tục hoàn thiện vấn đề này, Việt Nam đã ban hành Luật Dữ liệu năm 2024, Nghị định số 165/2025/NĐ-CP. Đặc biệt, Luật Bảo vệ dữ liệu cá nhân năm 2025 và mới đây nhất là Nghị định số 356/2025/NĐ-CP ra đời đã tạo nền tảng pháp lý vững chắc hơn, khắc phục tình trạng chồng chéo và thiếu đồng bộ trước đây. Sự kết hợp giữa các văn bản này kỳ vọng sẽ hình thành một hạ tầng pháp lý thống nhất và toàn diện cho quản trị dữ liệu tại Việt Nam, vừa bảo đảm mục tiêu bảo vệ an ninh - chủ quyền dữ liệu, vừa tạo thuận lợi cho tiến trình chuyển đổi số và phát triển kinh tế số của quốc gia.

1.1. Phạm vi áp dụng của dữ liệu chuyển giao

Trước đây, khoản 2 Điều 14 của Nghị định số 13/2023/NĐ-CP đã ghi nhận: *"chuyển dữ liệu cá nhân ra nước ngoài là hoạt động sử dụng không gian mạng, thiết bị, phương tiện điện tử hoặc các hình thức khác chuyển dữ liệu cá nhân của công dân Việt Nam tới một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc sử dụng một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam để xử lý dữ liệu cá nhân của công dân Việt Nam"*. Như vậy, phạm vi dữ liệu được chuyển giao trong căn cứ pháp lý nói trên đó chính là *"dữ liệu cá nhân của công dân Việt Nam"*. Cách tiếp cận này phản ánh quan niệm truyền thống về chủ quyền quốc gia gắn liền với quốc tịch, theo đó Nhà nước có nghĩa vụ bảo vệ công dân của mình ở bất cứ nơi đâu họ sinh sống, vì vậy, các dữ liệu chuyển giao ra nước ngoài chỉ được áp dụng đối với dữ liệu thuộc về công dân Việt Nam mà không ghi nhận với dữ liệu của công dân thuộc quốc gia khác.

Trong khi đó, các văn bản pháp luật gần đây bao gồm Luật Dữ liệu năm 2024, Nghị định số 165/2025/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định số 356/2025/NĐ-CP đã chuyển sang điều chỉnh phạm vi dữ liệu chuyển giao xuyên biên giới dưới góc nhìn lãnh thổ. Cụ thể, đối tượng điều chỉnh được xác

định dựa trên việc thu thập, lưu trữ, xử lý dữ liệu cá nhân diễn ra trên lãnh thổ Việt Nam, bất kể chủ thể dữ liệu là công dân Việt Nam hay người nước ngoài. Sự thay đổi này không chỉ đơn thuần là kỹ thuật lập pháp nhằm điều chỉnh phạm vi dữ liệu mà còn thể hiện sự phát triển mang tính chất bản chất trong quản trị dữ liệu hiện đại, hướng tới tiệm cận các chuẩn mực quốc tế. Điều này còn được thể hiện rõ trong cơ chế đánh giá tác động chuyển giao dữ liệu. Trước đây, theo Nghị định số 13/2023/NĐ-CP, chỉ các trường hợp chuyển dữ liệu cá nhân của công dân Việt Nam ra nước ngoài mới bắt buộc phải lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài. Tuy nhiên, Nghị định số 165/2025/NĐ-CP với tư cách là văn bản hướng dẫn thi hành Luật Dữ liệu năm 2024 đã thay đổi cách tiếp cận khi đưa ra các yêu cầu phân tầng dữ liệu cụ thể hơn, dựa trên "dữ liệu cốt lõi" và "dữ liệu quan trọng", nhấn mạnh tới tác động đối với an ninh quốc gia hơn là yếu tố quốc tịch của chủ thể dữ liệu. Có thể thấy rằng, sự chuyển dịch này phản ánh xu hướng cân bằng giữa bảo đảm chủ quyền dữ liệu quốc gia và phù hợp với thông lệ quốc tế. Các quy định này tạo điều kiện cho Việt Nam vừa bảo vệ lợi ích an ninh quốc gia, vừa tạo môi trường pháp lý cởi mở hơn cho dòng chảy dữ liệu toàn cầu, qua đó hỗ trợ tiến trình chuyển đổi số và hội nhập kinh tế quốc tế. Lý do của sự thay đổi này có thể được thúc đẩy bởi hai yếu tố chính:

Thứ nhất, quá trình số hóa diễn ra mạnh mẽ trên phạm vi toàn cầu. Trong môi trường số, ranh giới quốc gia cũng như quốc tịch ngày càng trở nên mờ nhạt. Dữ liệu được tạo ra, xử lý và lưu trữ xuyên biên giới một cách liên tục khiến cho việc xác định quốc tịch của chủ thể dữ liệu trở nên không thực tế, thậm chí bất khả thi. Về thực tiễn, dữ liệu cá nhân do người nước ngoài cư trú tại Việt Nam tạo ra cũng có thể tiềm ẩn nguy cơ và hệ quả đối với an ninh quốc gia tương đương với dữ liệu của công dân Việt Nam. Hơn nữa, cách tiếp cận dựa trên quốc tịch cũng tạo ra gánh nặng hành chính cũng như những lỗ hổng pháp lý trong bối cảnh điện toán đám mây và các nền tảng xuyên quốc gia phát triển mạnh.

Thứ hai, ảnh hưởng từ các quy định pháp luật quốc tế. Quy định bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu với tư cách là một trong những văn bản được xem là tiêu chuẩn trong bảo vệ dữ liệu cá nhân trên toàn thế giới đã áp dụng cách tiếp cận lãnh thổ, bảo vệ mọi dữ liệu cá nhân được xử lý trong phạm vi Khu vực kinh tế châu Âu (EEA) mà không phân biệt quốc tịch. Những cải cách pháp luật gần đây của Việt Nam cho thấy nỗ lực hài hòa với thông lệ quốc tế, đồng thời mở ra khả năng tăng cường hợp tác trong nền kinh tế số xuyên biên giới.

1.2. Điều kiện chuyển giao dữ liệu xuyên biên giới

Pháp luật Việt Nam hiện nay thiết lập một cơ chế kiểm soát tập trung và thống nhất đối với việc chuyển giao dữ liệu xuyên biên giới, trong đó công cụ chính là yêu cầu báo cáo đánh giá tác động của việc chuyển dữ liệu.

Trước đây, theo Điều 25 Nghị định số 13/2023/NĐ-CP, mọi hoạt động chuyển dữ liệu cá nhân ra nước ngoài đều phải kèm theo *"hồ sơ đánh giá tác động việc chuyển dữ liệu cá nhân ra nước ngoài"*. Hồ sơ này phải được gửi cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an trong thời hạn 60 ngày kể từ ngày bắt đầu xử lý dữ liệu, không phân biệt dữ liệu được chuyển sang quốc gia nào. Cơ chế này phản ánh cách tiếp cận chặt chẽ và tập trung, khi cơ quan nhà nước thuộc Bộ Công an giữ vai trò giám sát mọi trường

hợp chuyển giao dữ liệu. Luật Bảo vệ dữ liệu cá nhân năm 2025 kế thừa nguyên tắc nêu trên, song có sự điều chỉnh về thời điểm báo cáo khi khoản 2 Điều 20 quy định hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới phải được nộp trong vòng 60 ngày kể từ ngày chuyển dữ liệu. Sự điều chỉnh này là hoàn toàn hợp lý xuất phát từ sự khác nhau về bản chất của thời điểm chuyển dữ liệu và thời điểm xử lý dữ liệu. Trong thực tiễn, hoạt động xử lý dữ liệu là một chuỗi hành vi bao gồm thu thập, lưu trữ, phân tích, sử dụng, truyền tải và nhiều hoạt động trung gian khác; do đó rất khó xác định chính xác "mốc xử lý" nào được dùng làm điểm khởi đầu tính thời hạn 60 ngày. Ngược lại, hoạt động chuyển dữ liệu là một sự kiện pháp lý có tính thống nhất, xác định được bằng thời điểm kết nối, truyền dẫn trên hệ thống kỹ thuật. Việc lấy cột mốc chuyển dữ liệu làm thời điểm tính thời hạn 60 ngày từ đó giúp tăng tính minh bạch, giảm thiểu tranh chấp và loại bỏ sự tùy nghi trong diễn giải các quy định pháp luật.

Luật Dữ liệu năm 2024 đưa ra nguyên tắc chung cho chuyển dữ liệu xuyên biên giới tại khoản 3 Điều 23: *"phải bảo đảm quốc phòng, an ninh, bảo vệ lợi ích quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của chủ thể dữ liệu, chủ sở hữu dữ liệu theo quy định của pháp luật Việt Nam và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên"*. Như vậy, Luật Dữ liệu đã yêu cầu việc chuyển dữ liệu xuyên biên giới phải phù hợp với bảo vệ lợi ích công cộng cũng như lợi ích của hai chủ thể có liên quan trực tiếp đến dữ liệu chuyển giao đó là chủ thể dữ liệu, chủ sở hữu dữ liệu. Ngoài ra, Luật Dữ liệu năm 2024 và Nghị định số 165/2025/NĐ-CP đã xây dựng cơ chế giám sát riêng biệt đối với hai loại dữ liệu đặc thù là "dữ liệu quan trọng" và "dữ liệu cốt lõi". Đối với cả hai loại dữ liệu này, khoản 5 và khoản 6 Điều 12 yêu cầu báo cáo đánh giá tác động phải được thực hiện trước khi chuyển giao dữ liệu xuyên biên giới. Điều này đánh dấu một bước chuyển quan trọng từ cơ chế báo cáo mang tính hậu kiểm sang cơ chế giám sát tiền kiểm. Quy định này xuất phát từ mức độ ảnh hưởng cao mà những loại dữ liệu này có thể tạo ra so với dữ liệu thông thường khi có thể tác động hoặc trực tiếp tác động đến *"quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng"*[1]. Đặc biệt, riêng với các dữ liệu cốt lõi (ví dụ như dữ liệu biên giới quốc gia, chủ quyền lãnh thổ, dữ liệu về hoạt động công nghiệp quốc phòng, an ninh chưa công khai...[2]), việc chuyển giao chỉ được tiến hành sau khi cơ quan nhà nước có thẩm quyền phê duyệt trước. Như vậy, đối với dữ liệu quan trọng, cho dù phải thực hiện báo cáo tác động trước khi chuyển giao nhưng báo cáo này vẫn chỉ mang tính chất thông báo chứ không quyết định tới hoạt động chuyển giao. Còn với dữ liệu cốt lõi, việc báo cáo còn mang ý nghĩa phải có sự chấp thuận bắt buộc từ cơ quan có thẩm quyền, nếu không việc chuyển giao sẽ không được phép diễn ra. Đồng thời, cần lưu ý rằng, bản thân các dữ liệu quan trọng, dữ liệu cốt lõi cũng có thể là các dữ liệu cá nhân nên có thể chịu sự điều chỉnh của cả Luật Dữ liệu năm 2024, Nghị định số 165/2025/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định số 356/2025/NĐ-CP. Về điểm này, khoản 2 Điều 42 Nghị định số 356/2025/NĐ-CP cũng đã đưa ra nguyên tắc áp dụng cụ thể, theo đó khi chuyển giao dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới là dữ liệu cá nhân thì sẽ ưu tiên áp dụng các quy định pháp luật về bảo vệ dữ liệu cá nhân, tức là Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị

định số 356/2025/NĐ-CP. Quy định này hoàn toàn hợp lý vì cần áp dụng thống nhất cơ chế đối với dữ liệu cá nhân trong các văn bản pháp luật chuyên biệt chứ không phải là các văn bản pháp luật về dữ liệu nói chung.

Bên cạnh đó, khoản 3 Điều 12 Nghị định số 165/2025/NĐ-CP còn đưa ra nội dung liên quan đến văn bản giao kết giữa bên chuyển dữ liệu và bên nhận dữ liệu phải đáp ứng những yêu cầu bắt buộc về mục đích, phương pháp, phạm vi xuất dữ liệu, xử lý dữ liệu, địa điểm và thời gian lưu trữ dữ liệu, các biện pháp bảo vệ dữ liệu mà bên nhận dữ liệu sử dụng... Quy định này cho thấy pháp luật đã nhận diện và thậm chí kiểm soát cả nội dung nằm trong thỏa thuận giữa các bên liên quan đến việc chuyển dữ liệu nhằm bảo đảm mức độ an toàn cao nhất đối với dữ liệu được chuyển giao. So sánh với các biện pháp bảo vệ mà GDPR đã đưa ra thì có thể nhận thấy sự tương đồng nhất định giữa văn bản giao kết về chuyển giao dữ liệu này với hệ thống điều khoản hợp đồng mẫu (Standard Contractual Clauses – SCC) ghi nhận tại khoản 2 Điều 46 của GDPR. Tuy nhiên, sự khác biệt cơ bản đó là hệ thống SCC cho phép cơ quan có thẩm quyền can thiệp trực tiếp một cách mạnh mẽ vào sự thỏa thuận giữa các bên tham gia quan hệ chuyển giao dữ liệu, bắt buộc các chủ thể này phải tuân thủ theo ý chí của cơ quan soạn thảo là Ủy ban châu Âu. Điều này cho thấy quan điểm của GDPR đặt yếu tố bảo vệ quyền riêng tư của chủ thể dữ liệu lên ưu tiên hàng đầu, thậm chí cao hơn cả sự tự do ý chí của bên chuyển giao dữ liệu và bên nhận dữ liệu. Tư duy lập pháp này xuất phát từ mục tiêu xây dựng ban đầu của GDPR, vốn dĩ tập trung vào bảo vệ những quyền cơ bản của cá nhân trong phạm vi Liên minh châu Âu[3]. Đối với Việt Nam, pháp luật mới chỉ can thiệp ở mức độ vừa phải vào thỏa thuận của các bên dưới dạng bắt buộc phải có những nội dung nhất định, còn lại vẫn tôn trọng các nội dung khác trong văn bản này. Quan điểm trên mặc dù có tính chất dung hòa giữa tự do ý chí trong thỏa thuận chuyển giao dữ liệu và bảo vệ sự an toàn của dữ liệu, nhưng đồng thời cũng thiếu đi sự bảo vệ một cách quyết liệt đối với quyền riêng tư của cá nhân từ dữ liệu của mình.

1.3. Các trường hợp ngoại lệ không phải đánh giá tác động chuyển giao dữ liệu cá nhân xuyên biên giới

Nghị định số 13/2023/NĐ-CP tại Điều 25 trước đây không đưa ra bất kỳ trường hợp ngoại lệ nào cho việc không phải đánh giá tác động chuyển dữ liệu ra nước ngoài. Điều đó có nghĩa là tất cả các trường hợp chuyển dữ liệu ra nước ngoài bắt buộc phải có hồ sơ đánh giá tác động để được xem là hợp pháp. Trong khi đó Nghị định số 165/2025/NĐ-CP tại khoản 11 Điều 12 đã đưa ra các trường hợp ngoại lệ không cần sự chấp thuận của cơ quan có thẩm quyền khi chuyển dữ liệu cốt lõi xuyên biên giới và chuyển dữ liệu quan trọng không cần thông báo cho cơ quan có thẩm quyền bao gồm: (1) Các tình huống khẩn cấp thực sự cần thiết để bảo vệ sức khỏe, tính mạng và tài sản của cá nhân cũng như thực hiện nhiệm vụ, nghĩa vụ theo quy định pháp luật; (2) Thực hiện quản lý nhân sự xuyên biên giới theo quy tắc, quy chế lao động và thỏa ước lao động tập thể theo quy định của pháp luật; (3) Trường hợp thực sự cần thiết phải cung cấp dữ liệu nhằm mục đích ký kết hoặc thực hiện hợp đồng, bao gồm trường hợp hợp đồng liên quan đến vận chuyển xuyên biên giới, hậu cần, chuyển tiền, thanh toán, mở tài khoản ngân hàng và khách sạn, xin thị thực, dịch vụ kiểm tra. Khoản 6 Điều 20

của Luật Bảo vệ dữ liệu cá nhân năm 2025 tiếp tục ghi nhận các trường hợp không cần thực hiện quy định về đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới như việc chuyển dữ liệu cá nhân xuyên biên giới của cơ quan nhà nước có thẩm quyền; cơ quan, tổ chức lưu trữ dữ liệu cá nhân của người lao động thuộc cơ quan, tổ chức đó trên dịch vụ điện toán đám mây; chủ thể dữ liệu cá nhân tự chuyển dữ liệu cá nhân của mình xuyên biên giới; và các trường hợp khác theo quy định của Chính phủ. Bên cạnh đó, khoản 3 Điều 17 của Nghị định số 356/2025/NĐ-CP đã bổ sung thêm các trường hợp không phải tiến hành đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới như hoạt động báo chí, truyền thông theo quy định của pháp luật; việc chuyển dữ liệu cá nhân xuyên biên giới đã được công khai theo quy định của pháp luật.

Có thể thấy, thông qua sự xuất hiện ban đầu của Nghị định số 13/2023/NĐ-CP cho đến khi các văn bản pháp luật gần đây ra đời thay thế, đã có sự thay đổi tư duy lập pháp đáng kể liên quan đến việc chuyển giao dữ liệu xuyên biên giới từ mô hình kiểm soát tuyệt đối sang mô hình kiểm soát có điều kiện. Nghị định số 13/2023/NĐ-CP được ban hành trong giai đoạn đầu hình thành khung pháp luật về bảo vệ dữ liệu cá nhân tại Việt Nam. Với tư cách là văn bản tiên phong về vấn đề này, Nghị định số 13/2023/NĐ-CP vẫn chịu sự ảnh hưởng mạnh mẽ từ yêu cầu bảo đảm an ninh mạng và chủ quyền dữ liệu nói chung. Vì thế, trước những lo ngại về nguy cơ "chảy máu dữ liệu" ra nước ngoài, các nhà làm luật Việt Nam khi đó đã lựa chọn phương án an toàn khi thiết kế quy định chặt chẽ, buộc mọi chủ thể phải trải qua thủ tục đánh giá tác động. Đặc biệt khi Nghị định số 13/2023/NĐ-CP mới chỉ là văn bản ở cấp độ nghị định, thể hiện tính chất thí điểm và để xã hội làm quen với vấn đề bảo vệ dữ liệu cá nhân nói chung. Tuy nhiên, bối cảnh hiện nay đã thay đổi đáng kể khi Việt Nam đang có những động thái tích cực tham gia các hiệp định kinh tế số như Hiệp định Đối tác kinh tế số (DEPA). Những cam kết này khuyến khích tự do lưu chuyển dữ liệu xuyên biên giới và thúc đẩy nền kinh tế số phát triển, do vậy việc tiếp tục duy trì những rào cản pháp lý quá mức đối với chuyển giao dữ liệu dữ liệu sẽ không còn phù hợp. Bên cạnh đó, sự thay đổi trong cách tiếp cận của Việt Nam cũng cần được đặt trong bối cảnh so sánh quốc tế. Quy định của Liên minh châu Âu tại Điều 49 GDPR cho phép một số ngoại lệ đối với việc chuyển dữ liệu, ví dụ như bảo vệ lợi ích quan trọng của chủ thể dữ liệu hoặc dựa trên sự đồng ý rõ ràng của chủ thể dữ liệu, cần thiết để thực hiện hợp đồng... Đối với Trung Quốc, Cục An ninh mạng của quốc gia này vào ngày 22/03/2024 đã ban hành Quy định về thúc đẩy và điều chỉnh dòng chảy dữ liệu xuyên biên giới (Regulations on Promoting and Regulating Cross-Border Data Flows). Trong đó quy định tại Điều 5 cũng ghi nhận các ngoại lệ không cần đánh giá an ninh xuất khẩu dữ liệu bao gồm trường hợp cần thiết để giao kết hoặc thực hiện hợp đồng mà chủ thể dữ liệu là một bên trong đó; cần thiết để chuyển thông tin cá nhân của người lao động trong hoạt động quản lý nhân sự; các trường hợp khẩn cấp để bảo vệ tính mạng, sức khỏe, tài sản của cá nhân hoặc số lượng dữ liệu cá nhân cơ bản dưới 100.000 đơn vị[4]. Có thể thấy rằng, Nghị định số 13/2023/NĐ-CP với cách tiếp cận tuyệt đối, đã đứng ngoài xu hướng này. Chỉ đến khi Luật Dữ liệu năm 2024 và Luật Bảo vệ dữ liệu cá nhân năm 2025 được ban hành, Việt Nam mới chính thức nội luật hóa các ngoại lệ, qua đó tiệm cận hơn với

chuẩn mực quốc tế, giảm thiểu nguy cơ đứng ngoài cuộc chơi trong hoạt động của nền kinh tế số toàn cầu.

Đồng thời, cách tiếp cận của Việt Nam cũng phản ánh mô hình định hướng quản lý nhà nước nhằm cân bằng giữa việc bảo vệ lợi ích chủ thể dữ liệu với những thực tế quản trị và phát triển kinh tế. Cụ thể, việc áp dụng ngoại lệ tương đối rộng là "các trường hợp khác theo quy định của Chính phủ" đã tạo ra một cơ chế thích ứng cho phép phản ứng nhanh trước các tiến bộ công nghệ và mô hình kinh doanh mới mà không cần sửa đổi những văn bản pháp luật hiện hành. Tính linh hoạt này đặc biệt cần thiết đối với nền kinh tế số đang trỗi dậy của Việt Nam, nơi mà các quy định quá cứng nhắc có thể kìm hãm tính đổi mới sáng tạo.

2. Hoàn thiện quy định pháp luật Việt Nam về chuyển giao dữ liệu cá nhân xuyên biên giới

2.1. Bổ sung hệ thống điều khoản hợp đồng mẫu giữa bên chuyển dữ liệu và bên nhận dữ liệu

Một trong những công cụ bảo vệ dữ liệu nổi bật nhất của GDPR trong việc tạo thuận lợi cho hoạt động chuyển dữ liệu xuyên biên giới là hệ thống điều khoản hợp đồng mẫu (Standard Contractual Clauses – SCCs) do Ủy ban châu Âu ban hành năm 2021. Cơ chế này cung cấp bốn mô-đun cụ thể: Mô-đun 1 (bên kiểm soát – bên kiểm soát), Mô-đun 2 (bên kiểm soát – bên xử lý), Mô-đun 3 (bên xử lý – bên xử lý) và Mô-đun 4 (bên xử lý – bên kiểm soát), từ đó cho phép các chủ thể lựa chọn mẫu hợp đồng phù hợp với bản chất quan hệ hợp đồng dữ liệu của mình[5].

Trong khi đó, Việt Nam hiện nay chưa xây dựng một cơ chế tương tự. Do thiếu hướng dẫn chi tiết, doanh nghiệp được phép tự soạn thảo điều khoản bảo vệ dữ liệu trong hợp đồng, dẫn đến hai hệ quả: (i) Nhà nước khó can thiệp hiệu quả vào nội dung các thỏa thuận dữ liệu giữa các chủ thể và (ii) Khả năng bảo vệ dữ liệu bị suy giảm do thiếu những điều khoản chuẩn hóa và được thẩm định về mặt pháp lý. Cụ thể, khoản 3 Điều 12 Nghị định số 165/2025/NĐ-CP chỉ yêu cầu rằng "văn bản thỏa thuận giữa bên chuyển và bên nhận dữ liệu" phải xác định rõ mục đích, phương thức, biện pháp bảo vệ và trách nhiệm của các bên, song không đưa ra mẫu hợp đồng hay hướng dẫn cụ thể.

Để khắc phục khoảng trống này, Việt Nam nên phát triển hệ thống điều khoản hợp đồng mẫu riêng theo mô hình mô-đun của EU, gồm bốn mô-đun tương ứng. Tuy nhiên, bên cạnh việc học hỏi từ GDPR, hệ thống này cần được tích hợp các yếu tố đặc thù của Việt Nam, chẳng hạn như yêu cầu riêng biệt đối với dữ liệu cốt lõi, dữ liệu quan trọng cũng như nghĩa vụ báo cáo đối với cơ quan quản lý nhà nước có thẩm quyền. Một cơ chế điều khoản hợp đồng mẫu như vậy sẽ mang lại lợi ích kép khi vừa giảm chi phí tuân thủ cho doanh nghiệp thông qua các mẫu hợp đồng đã được chuẩn hóa và thẩm định pháp lý, vừa nâng cao hiệu quả bảo vệ dữ liệu nhờ các điều khoản được thiết kế chuyên nghiệp và thường xuyên cập nhật để thích ứng với tiến bộ công nghệ.

2.2. Bổ sung yêu cầu đánh giá chi tiết hệ thống pháp luật quốc gia tiếp nhận dữ liệu

Một hạn chế lớn trong hệ thống pháp luật Việt Nam về chuyển dữ liệu xuyên biên giới (bao gồm: Luật Dữ liệu năm 2024, Nghị định số 165/2025/NĐ-CP, Luật Bảo

vệ dữ liệu cá nhân năm 2025 và Nghị định số 356/2025/NĐ-CP) đó chính là thiếu yêu cầu đánh giá chi tiết hệ thống pháp luật của quốc gia hoặc vùng lãnh thổ tiếp nhận dữ liệu. Cụ thể, cả Nghị định số 165/2025/NĐ-CP[6] và Nghị định số 356/2025/NĐ-CP[7] đều không yêu cầu bất kỳ hình thức đánh giá pháp luật nào tại quốc gia tiếp nhận. So sánh với GDPR có thể thấy rằng, cơ chế quyết định mức độ đầy đủ (adequacy decision) được coi là tiêu chuẩn ưu tiên hàng đầu trong số các công cụ chuyển dữ liệu xuyên biên giới theo GDPR. Cơ chế này cho phép dòng chảy tự do của dữ liệu cá nhân từ Liên minh châu Âu sang các quốc gia thứ ba được lưu thông mà không cần thêm bất kỳ biện pháp bảo vệ bổ sung nào. Theo Điều 45 của GDPR, Ủy ban châu Âu có thẩm quyền xác định liệu một quốc gia thứ ba có "bảo đảm mức độ bảo vệ đầy đủ" hay không, dựa trên việc đánh giá toàn diện các yếu tố pháp lý, thể chế và thực tiễn, ví dụ như tính chất tôn trọng nhân quyền và các quyền tự do cơ bản, sự tồn tại và hoạt động hiệu quả của các cơ quan giám sát độc lập cũng như các cam kết quốc tế mà quốc gia đó tham gia. Việc thiếu vắng quy định về đánh giá hệ thống pháp luật tại nơi nhận dữ liệu đang tạo ra khoảng trống của biện pháp pháp lý nhằm bảo đảm an toàn cho chủ thể dữ liệu khi dữ liệu của họ rời khỏi lãnh thổ Việt Nam. Trong bối cảnh quốc tế, yêu cầu đánh giá này đóng vai trò trung tâm nhằm bảo vệ dữ liệu cá nhân trước những khác biệt lớn giữa các hệ thống pháp luật. Do đó, Việt Nam cần bổ sung nghĩa vụ bắt buộc đối với bên xuất khẩu dữ liệu trong việc tiến hành đánh giá toàn diện khung pháp luật bảo vệ dữ liệu của quốc gia hoặc vùng lãnh thổ tiếp nhận. Báo cáo đánh giá này phải chứng minh rằng, bên tiếp nhận dữ liệu bảo đảm một mức độ bảo vệ nhất định đối với dữ liệu hoặc trong trường hợp không đạt được, phải có các biện pháp bổ sung phù hợp nhằm giảm thiểu rủi ro xuống mức chấp nhận được./.

---

[1] Khoản 6, 7 Điều 3 Luật Dữ liệu năm 2024.

[2] Danh mục Dữ liệu cốt lõi ban hành kèm Quyết định số 20/2025/QĐ-TTg ngày 01/07/2025 về ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi.

[3] Yeung, K. and Bygrave, L.A. (2022), *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, Regulation & Governance, 16: 137-155. https://doi.org/10.1111/rego.12401.

[4] Xem thêm tại: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, truy cập ngày 02/09/2025.

[5] European Commission, *New Standard Contractual Clauses – Questions and Answers overview*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en, truy cập ngày 27/07/2025.

[6] Mẫu số 02 - Báo cáo đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới ban hành kèm theo Nghị định số 165/2025/NĐ-CP.

[7] Mẫu số 09 - Báo cáo đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới ban hành kèm theo Nghị định số 356/2025/NĐ-CP.