MÂU THUẪN GIỮA YÊU CẦU NỘI ĐỊA HÓA DỮ LIỆU THEO LUẬT AN NINH MẠNG VỚI CAM KẾT VỀ LUỒNG DỮ LIỆU TỰ DO TRONG CPTPP

TRẦN QUYẾT THẮNG*

Bài viết phân tích xung đột pháp lý giữa yêu cầu nội địa hóa dữ liệu theo Luật An ninh mạng năm 2018 của Việt Nam và cam kết luồng dữ liệu tự do trong Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP). Khung pháp lý hiện tại của Việt Nam, với phạm vi rộng và cơ chế kích hoạt thiếu rõ ràng, khó được biện minh theo ngoại lệ an ninh quốc gia của CPTPP. Dựa trên phân tích quy phạm và so sánh với mô hình Singapore, Australia, bài viết đề xuất một lộ trình hài hòa hóa thực dụng: thu hẹp nội địa hóa bắt buộc chỉ đối với dữ liệu tối quan trọng về an ninh quốc gia, áp dụng khuôn khổ chuyển giao dữ liệu dựa trên trách nhiệm giải trình cho các loại dữ liệu còn lại. Giải pháp này cho phép Việt Nam bảo vệ lợi ích an ninh thiết yếu, tuân thủ nghĩa vụ quốc tế, thúc đẩy hội nhập và tăng trưởng bền vững trong kỷ nguyên số.

Từ khóa: *Nội địa hóa dữ liệu; Luật An ninh mạng; CPTPP; xung đột pháp lý; hài hòa hóa pháp luật.*

The article analyzes the legal conflict between data localization requirements under Vietnam's 2018 Cybersecurity Law and commitments on free data flows in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Vietnam's current legal framework, with its broad scope and unclear triggering mechanisms, is difficult to justify under the national security exceptions of the CPTPP. Based on normative analysis and comparisons with Singapore's and Australia's models, the article proposes a pragmatic roadmap for harmonization: narrowing mandatory data localization to only data of critical importance to national security, and applying an accountability-based data transfer framework to other categories of data. This solution enables Vietnam to safeguard essential security interests, comply with international obligations, and promote integration and sustainable growth in the digital era.

Keywords: *Data localization; Cybersecurity Law; CPTPP; legal conflict; legal harmonization.*

NGÀY NHẬN: 19/12/2025 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 25/3/2026 NGÀY DUYỆT: 17/4/2026

DOI: https://doi.org/10.59394/qlnn.363.2026.1483

1. Đặt vấn đề

Trong kỷ nguyên số, dữ liệu đã trở thành một nguồn tài nguyên chiến lược, là nền tảng cho sự phát triển kinh tế và đổi mới sáng tạo. Tuy nhiên, cách thức quản trị nguồn tài nguyên này đang tạo ra một sự phân đôi sâu sắc trên toàn cầu. Một bên là mô hình thúc đẩy luồng dữ liệu tự do xuyên

* *TS, Học viện Hành chính và Quản trị công*

biên giới, được xem là động lực cốt lõi cho tăng trưởng kinh tế và hiệu quả hoạt động của các doanh nghiệp đa quốc gia. Mô hình này được thể chế hóa trong các hiệp định thương mại tự do thế hệ mới, điển hình là Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), với những cam kết mạnh mẽ nhằm gỡ bỏ các rào cản đối với thương mại số.

Ở phía đối diện là mô hình nhấn mạnh chủ quyền dữ liệu và an ninh quốc gia, với công cụ chính sách chủ đạo là yêu cầu nội địa hóa dữ liệu. Cách tiếp cận này coi việc lưu trữ và xử lý dữ liệu trong phạm vi lãnh thổ quốc gia là một biện pháp thiết yếu để nhà nước thực thi quyền kiểm soát, bảo vệ an ninh và các lợi ích công cộng khác. Nhiều quốc gia, với những mức độ khác nhau, đã áp dụng các quy định này, tạo ra một bối cảnh pháp lý phức tạp và phân mảnh trên toàn cầu.

Việt Nam là thành viên tích cực của CPTPP và nhiều hiệp định thương mại tự do khác, Việt Nam đã cam kết hội nhập sâu rộng vào nền kinh tế toàn cầu. Đồng thời, với việc ban hành *Luật An ninh mạng* năm 2018 và các văn bản hướng dẫn, Việt Nam cũng thể hiện một cách tiếp cận quyết đoán trong việc khẳng định chủ quyền trên không gian mạng và bảo vệ an ninh quốc gia thông qua các yêu cầu nghiêm ngặt về nội địa hóa dữ liệu. Chính sách hai hướng này đặt Việt Nam vào trung tâm của một cuộc xung đột pháp lý và triết lý quản trị, nơi các nghĩa vụ hội nhập quốc tế va chạm với các ưu tiên an ninh nội địa. Việc phân tích và tìm kiếm giải pháp cho mâu thuẫn này không chỉ có ý nghĩa đối với Việt Nam mà còn cung cấp những bài học kinh nghiệm quý giá cho các quốc gia khác đang phải đối mặt với thách thức tương tự.

2. Nội dung của pháp luật Việt Nam và CPTTP về nội địa hóa dữ liệu

2.1. Yêu cầu nội địa hóa dữ liệu

Khung pháp lý quản trị dữ liệu của Việt Nam được định hình chủ yếu bởi *Luật An ninh mạng* năm 2018 (có hiệu lực từ ngày 01/01/2019) và được cụ thể hóa qua Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 (hiệu lực từ ngày 01/10/2022). Mặc dù *Luật* có quy định về nội địa hóa từ năm 2019, nhưng chỉ khi Nghị định số 53/2022/NĐ-CP ra đời, các yêu cầu mới từ lý thuyết chuyển thành nghĩa vụ tuân thủ cấp bách cho cộng đồng doanh nghiệp.

Phạm vi áp dụng của các yêu cầu nội địa hóa rất rộng, bao trùm ba loại dữ liệu chính: (1) Thông tin cá nhân người dùng dịch vụ tại Việt Nam; (2) Dữ liệu do người dùng tạo ra, bao gồm tên tài khoản, thống kê sử dụng, thông tin thanh toán, địa chỉ email, IP đăng nhập và số điện thoại; (3) Dữ liệu mối quan hệ, gồm danh sách bạn bè và các nhóm kết nối. Phạm trù này bao phủ gần như toàn bộ hoạt động trên các nền tảng số hiện đại.

Đối với đối tượng áp dụng, các doanh nghiệp trong nước, kể cả doanh nghiệp có vốn nước ngoài (FIEs) phải lưu trữ dữ liệu nếu hoạt động trong các lĩnh vực xác định. Đối với doanh nghiệp nước ngoài không có hiện diện pháp lý tại Việt Nam, yêu cầu nội địa hóa và đặt chi nhánh tại Việt Nam chỉ kích hoạt khi hội đủ hai điều kiện: hoạt động trong các lĩnh vực quy định (mạng xã hội, thương mại điện tử, thanh toán trực tuyến) và quan trọng nhất, bị Bộ Công an xác định là vi phạm pháp luật Việt Nam nhưng không chấp hành hoặc cản trở các biện pháp bảo vệ an ninh mạng. Sau khi nhận quyết định của Bộ trưởng Bộ Công an, doanh nghiệp có 12 tháng hoàn thành[1].

Cơ chế kích hoạt này tiết lộ sự lồng ghép giữa yêu cầu kỹ thuật (lưu trữ dữ liệu) và tuân thủ nội dung. Việc đặt điều kiện "không chấp hành" yêu cầu cơ quan chức năng biến nội địa hóa thành công cụ chế tài và đòn bẩy thực thi pháp luật, chứ không phải yêu cầu kỹ thuật thuần túy. Cách tiếp cận này tương đồng với mô hình Trung Quốc, sử dụng biện pháp kinh tế và kỹ thuật cho mục tiêu chính trị về kiểm soát thông tin và khẳng định chủ quyền không gian mạng[2].

Mục tiêu chính của *Luật* là bảo vệ an ninh quốc gia, trật tự xã hội và quyền lợi hợp pháp. *Luật* dành nhiều điều khoản ngăn chặn các hành vi bị cấm, như: tuyên truyền chống Nhà nước, kích động bạo loạn, làm nhục, vu khống hoặc đăng tải thông tin sai sự thật. Yêu cầu lưu trữ dữ liệu được xem là cần thiết để các cơ quan chức năng Việt Nam truy cập, xác minh và xử lý vi phạm kịp thời, thay vì phụ thuộc vào thủ tục tương trợ tư pháp quốc tế phức tạp và tốn thời gian. Lập luận này nhấn mạnh rằng, dữ liệu lưu trữ ở nước ngoài, như: Hồng Kông (Trung Quốc), Singapore gây khó khăn cho điều tra và bảo vệ an ninh quốc gia, từ đó, biện minh cho sự cần thiết của các yêu cầu nội địa hóa[3].

2.2. Các cam kết về luồng dữ liệu tự do trong CPTPP

CPTPP được công nhận rộng rãi là một hiệp định thương mại tự do thế hệ mới, với các tiêu chuẩn cao và phạm vi cam kết sâu rộng. Trong đó, Chương 14 về thương mại điện tử được xem là một "tiêu chuẩn vàng" cho các quy tắc thương mại số toàn cầu. Trong đó, mục tiêu là thúc đẩy tăng trưởng kinh tế thông qua việc tạo điều kiện thuận lợi cho thương mại điện tử, bảo vệ người tiêu dùng và quan trọng nhất là ngăn chặn các quốc gia thành viên dựng lên các rào cản không cần thiết đối với luồng dữ liệu xuyên biên giới. Triết lý nền tảng của Chương 14 hoàn toàn trái ngược với triết lý kiểm soát của *Luật An ninh mạng* Việt Nam, tạo ra một điểm xung đột trực tiếp.

Hai điều khoản trong Chương 14 tạo thành nền tảng pháp lý vững chắc cho nguyên tắc luồng dữ liệu tự do và cấm nội địa hóa gồm:

Thứ nhất, Điều 14.13 (địa điểm của cơ sở hạ tầng công nghệ thông tin) quy định: "Không bên nào được yêu cầu một đối tượng được bảo hộ phải sử dụng hoặc đặt cơ sở hạ tầng công nghệ thông tin tại lãnh thổ của bên đó như một điều kiện để tiến hành hoạt động kinh doanh tại lãnh thổ đó". Đây là một lệnh cấm trực tiếp và không mơ hồ đối với các yêu cầu nội địa hóa dữ liệu bắt buộc. Yêu cầu của Việt Nam buộc doanh nghiệp phải lưu trữ dữ liệu tại Việt Nam rõ ràng đi ngược lại với tinh thần và câu chữ của điều khoản này.

Thứ hai, để bổ trợ cho Điều 14.13, Điều 14.11 (chuyển giao thông tin xuyên biên giới bằng phương tiện điện tử) yêu cầu mỗi bên phải "cho phép việc chuyển giao thông tin xuyên biên giới bằng phương tiện điện tử... khi hoạt động này là để phục vụ cho việc tiến hành hoạt động kinh doanh của một đối tượng được bảo hộ". Nghĩa vụ "cho phép" này bảo đảm rằng, dữ liệu không chỉ được phép lưu trữ ở nước ngoài mà còn phải được di chuyển một cách tự do để phục vụ hoạt động kinh doanh.

Ngoài ra, CPTPP cũng dự liệu các "van an toàn" cho phép các quốc gia thành viên áp dụng các biện pháp cần thiết để bảo vệ các lợi ích công cộng quan trọng. Đây chính là các điều khoản mà Việt Nam có thể viện dẫn để biện minh cho *Luật An ninh mạng*.

Cả Điều 14.11 và 14.13 đều chứa một ngoại lệ cho phép một bên áp dụng các biện pháp không nhất quán với các nghĩa vụ này "để đạt được một mục tiêu chính sách công hợp pháp". Tuy nhiên, ngoại lệ này không phải là một "tấm séc trắng". Biện pháp đó phải thỏa mãn hai điều kiện nghiêm ngặt: *một là,* không được áp dụng theo cách tạo ra sự phân biệt đối xử tùy tiện, vô lý hoặc một sự hạn chế trá hình đối với thương mại; *hai là,* "không được áp đặt các hạn chế... lớn hơn mức cần thiết để đạt được mục tiêu đó". Vế thứ hai này chính là "bài kiểm tra tính cần thiết", một tiêu chuẩn rất cao và là trung tâm của các tranh luận pháp lý trong luật thương mại quốc tế[4].

CPTPP còn có một ngoại lệ chung về an ninh tại Điều 29.2. Đây là một ngoại lệ có phạm vi rộng, nhưng việc giải thích và áp

dụng cũng phải tuân thủ các nguyên tắc của luật pháp quốc tế, tránh lạm dụng để theo đuổi các mục tiêu bảo hộ.

Cấu trúc của CPTPP tạo ra một quy tắc mặc định là luồng dữ liệu tự do và đặt gánh nặng chứng minh lên bất kỳ quốc gia nào muốn đi chệch khỏi quy tắc đó. Toàn bộ cuộc tranh luận pháp lý không còn nằm ở câu hỏi "Liệu Việt Nam có lợi ích an ninh hợp pháp hay không?" Thay vào đó, chuyển sang câu hỏi khó khăn hơn: "Liệu biện pháp nội địa hóa dữ liệu trên diện rộng có phải là phương tiện ít hạn chế thương mại nhất trong số các phương tiện hợp lý có sẵn để bảo vệ lợi ích an ninh đó hay không?". Đây là một tiêu chuẩn pháp lý cao và là thách thức lớn đối với tính hợp pháp của *Luật An ninh mạng* Việt Nam trong khuôn khổ CPTPP.

3. Nội dung xung đột về quy định nội địa hóa dữ liệu giữa pháp luật Việt Nam và CPTPP

Khi đặt các quy định của *Luật An ninh mạng* năm 2018 và Nghị định số 53/2022/NĐ-CP bên cạnh các cam kết trong CPTPP, một sự mâu thuẫn pháp lý trực tiếp và rõ ràng sẽ hiện ra. Yêu cầu của Việt Nam buộc các doanh nghiệp phải lưu trữ các loại dữ liệu cụ thể trong nước và thậm chí thiết lập hiện diện thương mại là một sự vi phạm hiển nhiên đối với các nghĩa vụ tại Điều 14.11 và 14.13 của CPTPP.

Lập luận chính của phía Việt Nam là các quy định này nằm trong phạm vi ngoại lệ về an ninh quốc gia được cho phép bởi CPTPP. Lập luận này dựa trên quan điểm rằng, chủ quyền quốc gia trên không gian mạng là một lợi ích an ninh thiết yếu và việc kiểm soát dữ liệu là cần thiết để chống lại các mối đe dọa, như: thông tin sai lệch, tội phạm mạng và các hoạt động gây bất ổn chính trị. Việt Nam cũng chỉ ra rằng, nhiều quốc gia khác (bao gồm cả các thành viên WTO) và các nước phát triển cũng có các quy định tương tự về địa phương hóa dữ liệu[5].

Tuy nhiên, khi soi chiếu dưới lăng kính của luật thương mại quốc tế, lập luận này bộc lộ những điểm yếu đáng kể. "Bài kiểm tra tính cần thiết" trong ngoại lệ của CPTPP đòi hỏi quốc gia áp dụng biện pháp phải chứng minh rằng không có biện pháp thay thế nào khác, ít hạn chế thương mại hơn mà vẫn có thể đạt được mục tiêu chính sách tương tự một cách hiệu quả.

Luật An ninh mạng của Việt Nam, với phạm vi áp dụng rộng và các quy định mang tính bao trùm, khó có thể vượt qua được bài kiểm tra này. Bởi vì an ninh dữ liệu phụ thuộc vào các biện pháp kỹ thuật, quy trình quản lý, mã hóa và chuyên môn của nhà cung cấp, chứ không phải vị trí máy chủ. Việc buộc các công ty từ bỏ các nhà cung cấp đám mây toàn cầu hàng đầu với khả năng bảo mật tiên tiến để chuyển sang các nhà cung cấp trong nước ít kinh nghiệm hơn có thể làm suy yếu an ninh và tạo ra các "mục tiêu tập trung" dễ bị tấn công. Hơn nữa, sự tồn tại của các phương pháp thay thế ít gây rối loạn, như: tăng cường hợp tác thực thi pháp luật quốc tế, yêu cầu mã hóa mạnh hoặc áp dụng các mô hình chuyển giao dữ liệu có trách nhiệm giải trình làm suy yếu nghiêm trọng lập luận rằng, nội địa hóa trên diện rộng là "cần thiết". Đồng thời, việc gắn nghĩa vụ nội địa hóa với hành vi không tuân thủ các yêu cầu gỡ bỏ nội dung cho thấy, biện pháp này có thể bị xem là một công cụ thực thi pháp luật mang tính trừng phạt, chứ không phải là một biện pháp kỹ thuật để bảo vệ an ninh.

Các hiệp hội doanh nghiệp nước ngoài, như: Phòng Thương mại Hoa Kỳ (AmCham) và Phòng Thương mại châu Âu (EuroCham) đã đưa ra bốn mối quan ngại chính:

(1) Chi phí gia tăng và gián đoạn hoạt động. Yêu cầu nội địa hóa buộc các công ty phải chịu chi phí khổng lồ để xây dựng hoặc thuê trung tâm dữ liệu tại Việt Nam, phá vỡ các mô hình công nghệ thông tin tích hợp, toàn cầu hóa của các tập đoàn đa quốc gia.

(2) *Luật* này bị cho là làm giảm khả năng cạnh tranh và sức hấp dẫn đầu tư của Việt Nam. Một cuộc khảo sát của AmCham cho thấy, 61% công ty được hỏi sẽ ít có khả năng đầu tư vào Việt Nam hơn vì *Luật* này, và 89% cho rằng, nó sẽ làm cho nền kinh tế số kém cạnh tranh hơn[6].

(3) Sự không chắc chắn về pháp lý do thiếu các hướng dẫn chi tiết và các tiêu chí áp dụng mơ hồ, tạo ra một môi trường kinh doanh rủi ro, gây khó khăn cho các nhà đầu tư trong việc lập kế hoạch dài hạn.

(4) Các bên liên quan khẳng định rõ ràng rằng, *Luật* này có nguy cơ vi phạm các cam kết của Việt Nam không chỉ trong CPTPP mà còn trong WTO và Hiệp định Thương mại tự do Việt Nam-EU (EVFTA), có thể dẫn đến các vụ kiện pháp lý chống lại Việt Nam tại các cơ chế giải quyết tranh chấp quốc tế.

4. Kinh nghiệm và giải pháp hài hòa quy định pháp lý về nội địa hóa dữ liệu

Để giải quyết xung đột giữa an ninh và hội nhập, trước hết Việt Nam cần xem xét các mô hình quản trị dữ liệu của các quốc gia khác, đặc biệt là các thành viên CPTPP để rút ra những bài học và lộ trình khả thi.

Singapore và Australia cung cấp hai mô hình hiệu quả trong việc quản lý luồng dữ liệu xuyên biên giới, chứng minh việc bảo vệ dữ liệu mạnh mẽ hoàn toàn có thể tương thích với các nghĩa vụ thương mại quốc tế như CPTPP. Singapore, một trung tâm dữ liệu toàn cầu, không cấm chuyển dữ liệu ra nước ngoài mà áp dụng "nghĩa vụ hạn chế chuyển giao" theo *Luật Bảo vệ dữ liệu cá nhân* (PDPA). Điều này yêu cầu bên chuyển phải thực hiện các bước hợp lý để bảo đảm bên nhận nước ngoài cam kết bảo vệ dữ liệu theo tiêu chuẩn tương đương PDPA[7]. Các cơ chế để đáp ứng nghĩa vụ này rất linh hoạt, bao gồm: chuyển dữ liệu đến các quốc gia tương đương, sử dụng các điều khoản hợp đồng mẫu (SCCs), quy tắc ràng buộc của doanh nghiệp (BCRs) hoặc các khuôn khổ được công nhận như APEC CBPR. Cách tiếp cận này tập trung vào trách nhiệm giải trình của bên chuyển dữ liệu, cho phép luồng dữ liệu tự do cần thiết cho kinh doanh mà vẫn bảo đảm tiêu chuẩn bảo vệ cao.

Trong khi đó, Australia áp dụng cách tiếp cận dựa trên rủi ro. Quốc gia này không có luật nội địa hóa dữ liệu chung mà chỉ áp đặt các yêu cầu lưu trữ dữ liệu tại chỗ rất nghiêm ngặt đối với các loại dữ liệu cụ thể và nhạy cảm, nơi rủi ro được coi là cao nhất. Điển hình là hồ sơ sức khỏe điện tử ("My health record") hoặc dữ liệu liên quan đến cơ sở hạ tầng quan trọng theo Đạo luật An ninh Cơ sở hạ tầng quan trọng (SOCI Act). Đối với đa số dữ liệu thương mại và cá nhân khác, Australia cho phép chuyển giao xuyên biên giới miễn là tuân thủ Nguyên tắc về quyền riêng tư của Australia (APPs), tương tự như mô hình trách nhiệm giải trình của Singapore[8]. Cách tiếp cận có mục tiêu này chỉ áp dụng biện pháp hạn chế thương mại nhất (nội địa hóa) khi cần thiết để bảo vệ một lợi ích công cộng cực kỳ quan trọng, do đó dễ dàng vượt qua "bài kiểm tra tính cần thiết" của CPTPP. Cả hai quốc gia đều ưu tiên trách nhiệm giải trình hoặc áp dụng hạn chế có mục tiêu dựa trên rủi ro thay vì lệnh cấm chuyển giao dữ liệu trên diện rộng.

Dựa trên các phân tích pháp lý và bài học so sánh, Việt Nam có thể thực hiện các giải pháp sau:

Thứ nhất, sửa đổi và thu hẹp phạm vi nội địa hóa. Trước tiên cần sửa đổi Nghị định số 53/2022/NĐ-CP để xác định rõ ràng và thu hẹp phạm vi dữ liệu bắt buộc lưu trữ. Chỉ một danh mục rất hẹp gồm "dữ liệu tối quan trọng đối với an ninh quốc gia" (ví dụ: dữ liệu liên quan đến quốc phòng, hoạt động của các hệ thống hạ tầng trọng yếu, bí mật nhà nước) mới phải chịu yêu cầu nội địa hóa nghiêm ngặt. Cách tiếp cận này sẽ tương tự như mô hình dựa trên rủi ro của Australia và có khả năng cao hơn để được biện minh theo các ngoại lệ của CPTPP.

Thứ hai, đối với tất cả dữ liệu cá nhân và thương mại không được phân loại là "tối quan trọng", Việt Nam nên chuyển sang một khung pháp lý dựa trên trách nhiệm giải trình theo mô hình của Singapore. Điều này sẽ cho phép việc chuyển dữ liệu xuyên biên giới, với điều kiện các công ty phải sử dụng các cơ chế được phê duyệt (ví dụ: các điều khoản hợp đồng mẫu do Chính phủ ban hành, các chứng nhận quốc tế như APEC CBPR) để bảo đảm dữ liệu được bảo vệ ở nước ngoài theo tiêu chuẩn của Việt Nam. Điều này sẽ đáp ứng nhu cầu của doanh nghiệp trong khi vẫn duy trì sự bảo vệ dữ liệu.

Thứ ba, cần tăng cường tính minh bạch và thủ tục công bằng. Quy trình xác định dữ liệu nào là "tối quan trọng" hoặc quy trình thực thi các biện pháp an ninh cần phải được công khai, minh bạch với các tiêu chí rõ ràng. Các doanh nghiệp bị ảnh hưởng phải có quyền khiếu nại và được xét xử công bằng. Điều này làm giảm sự không chắc chắn về pháp lý vốn đang là một yếu tố cản trở đầu tư.

Thứ tư, cần tách bạch quản lý nội dung và nội địa hóa dữ liệu. Việc thực thi các quy định về nội dung trực tuyến bất hợp pháp nên được xử lý thông qua các cơ chế pháp lý khác (ví dụ: hợp tác với các nền tảng, các chế tài hiện có về xử phạt hành chính hoặc hình sự), thay vì sử dụng mối đe dọa nội địa hóa dữ liệu như một công cụ thực thi. Việc tách bạch này sẽ giúp *Luật An ninh mạng* tập trung hơn vào mục đích an ninh mạng kỹ thuật thuần túy, làm cho nó dễ dàng được biện minh hơn theo các ngoại lệ của CPTPP.

5. Kết luận

Từ kết quả phân tích cho thấy, *Luật An ninh mạng* năm 2018 và Nghị định số 53/2022/NĐ-CP, đặc biệt các quy định về nội địa hóa dữ liệu và hiện diện tại chỗ tạo ra xung đột đáng kể với nghĩa vụ theo CPTPP. Các yêu cầu này mâu thuẫn trực tiếp với điều khoản cấm nội địa hóa và thúc đẩy luồng dữ liệu tự do, trong khi lập luận dựa trên ngoại lệ an ninh quốc gia khó đáp ứng được các tiêu chuẩn về tính cần thiết và tương xứng trong luật thương mại quốc tế. Phạm vi áp dụng rộng và việc gắn nội địa hóa với quản lý nội dung khiến các biện pháp khó được coi là ít hạn chế thương mại nhất. Chính vì vậy, việc đề xuất một lộ trình hài hòa thực dụng: áp dụng nội địa hóa có mục tiêu, dựa trên rủi ro theo mô hình Australia cho một phạm vi rất hẹp dữ liệu tối quan trọng; đồng thời, triển khai khuôn khổ chuyển giao dữ liệu dựa trên trách nhiệm giải trình theo mô hình Singapore nhằm đạt "mục tiêu kép": bảo vệ an ninh thiết yếu để Việt Nam tuân thủ cam kết CPTPP, củng cố niềm tin nhà đầu tư và thúc đẩy kinh tế số❐

Chú thích:

1. Chính phủ (2022). *Nghị định số 53/2022/NĐ-CP quy định chi tiết một số điều của Luật An ninh mạng.*

2. Burri, M. (2021). *The Governance of Data and the CPTPP. In M. El-Agati & M. T. T. (Eds.).* The Trans-Pacific Partnership Agreement (CPTPP): A Commentary (pp. 345-368). Cambridge University Press.

3. EuroCham Vietnam. (2023). *Whitebook 2023: Trade & Investment Issues and Recommendations.* European Chamber of Commerce in Vietnam.

4. Geist, M. (2019). *The CPTPP and Digital Trade: A Canadian Perspective on the Data Localization, Cross-Border Data Flows, and Source Code Provisions.* Journal of International Economic Law, 22(1), tr. 85 - 105.

5. Greenleaf, G. (2019). *Vietnam's Cybersecurity Law 2018: A new data localisation giant.* Privacy Laws & Business International Report, 156, tr. 1 - 5.

6. AmCham Vietnam (2021). *Submission on the Draft Decree Guiding the Law on Cybersecurity.* American Chamber of Commerce in Vietnam.

7. Personal Data Protection Commission Singapore (2021). *Advisory Guidelines on the Personal Data Protection Act for Selected Topics.* https://www.pdpc.gov.sg, truy cập ngày 01/8/2025.

8. Australian Government (2018). *Security of Critical Infrastructure Act 2018.* Federal Register of Legislation.