PHÁP LUẬT VỀ CHỦ QUYỀN DỮ LIỆU SỐ TRONG MÔI TRƯỜNG ĐIỆN TOÁN ĐÁM MÂY: KINH NGHIỆM QUỐC TẾ VÀ HÀM Ý VỚI VIỆT NAM

MAI THỊ KIM SA
Hãng Luật Mai Thị Kim Sa
Mai Thi Kim Sa Law Firm
Email: sakimmai@gmail.com

Ngày nhận bài: 6/7/2026
Ngày sửa bài: 24/7/2026
Ngày duyệt đăng bài: 7/8/2026

Tóm tắt:

Bài viết tiếp cận chủ quyền dữ liệu số như năng lực pháp lý và kỹ thuật trong việc quyết định điều kiện truy cập, xử lý, chuyển giao, kiểm toán và bảo vệ dữ liệu, thay vì đồng nhất với nghĩa vụ lưu trữ trong nước. Bài viết so sánh mô hình của Liên minh châu Âu, Trung Quốc và Hoa Kỳ, sau đó đánh giá pháp luật Việt Nam theo Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025, Luật An ninh mạng năm 2025 và các văn bản liên quan. Việt Nam đã hình thành các cấu phần về phân loại dữ liệu, đánh giá tác động, kiểm soát chuyển dữ liệu xuyên biên giới và an ninh mạng. Tuy nhiên, pháp luật còn thiếu cơ chế chuyên biệt cho dịch vụ đám mây, quy tắc phối hợp giữa các luật và công cụ xử lý xung đột quyền tài phán. Bài viết đề xuất quản trị theo rủi ro, kết hợp kiểm soát pháp lý, kỹ thuật và quyền của chủ thể dữ liệu.

Từ khóa: *chủ quyền dữ liệu số, điện toán đám mây, dữ liệu xuyên biên giới, bản địa hóa dữ liệu, bảo vệ dữ liệu cá nhân*

Legal regulation of digital data sovereignty in cloud computing: International experience and lessons for Vietnam

Abstract:

Cloud computing weakens the traditional relationship between data, territory, and jurisdiction. This study conceptualizes digital data sovereignty as the legal and technical capacity to determine conditions governing data access, processing, transfer, auditing, and protection rather than equating sovereignty solely with domestic data-storage requirements. It compares regulatory approaches in the European Union, China, and the United States and evaluates Vietnam's framework under the 2024 Law on Data, the 2025 Law on Personal Data Protection, the 2025 Law on Cybersecurity, and related legislation. Vietnam has established mechanisms for data classification, impact assessment, cross-border data-transfer control, and cybersecurity. However, gaps remain in cloud-specific regulation, coordination among relevant laws, and mechanisms for resolving jurisdictional conflicts. The study recommends a risk-based governance approach integrating legal safeguards, technical controls, and data-subject rights.

Keywords: *digital data sovereignty, cloud computing, cross-border data flows, data localization, personal data protection*

1. Đặt vấn đề

Điện toán đám mây là hạ tầng quan trọng của kinh tế số. Theo NIST, đây là mô hình cho phép truy cập theo nhu cầu đến tài nguyên tính toán dùng chung, có thể cung cấp và thu hồi nhanh với chi phí quản trị thấp (Mell & Grance, 2011). Mô hình này giảm chi phí đầu tư và mở rộng linh hoạt, nhưng dữ liệu có thể được xử lý tại nhiều quốc gia dưới sự chi phối của các pháp nhân và hệ thống pháp luật khác nhau.

Vấn đề cốt lõi là quyền kiểm soát thực tế. Dữ liệu đặt trong nước vẫn có thể phụ thuộc vào phần mềm, khóa mã hóa hoặc tài khoản quản trị ở nước ngoài; dữ liệu đặt ngoài lãnh thổ vẫn có thể được kiểm soát nếu có quyền kiểm toán, hoàn trả, xóa và thực thi đối với nhà cung cấp. Đồng nhất chủ quyền với bản địa hóa có thể tăng chi phí nhưng không giải quyết được phụ thuộc công nghệ và quyền truy cập đặc quyền (Chander & Lê, 2015; Casalini & López González, 2019).

Chủ quyền số có thể chỉ quyền lực của nhà nước, khả năng tự chủ công nghệ hoặc quyền tự quyết của cá nhân (Couture & Toupin, 2019). Bài viết tiếp cận chủ quyền dữ liệu như khả năng kiểm soát có thể chứng minh được đối với vòng đời dữ liệu, sử dụng phân tích quy phạm và so sánh pháp luật để rút ra bài học cho Việt Nam.

2. Cơ sở lý luận về chủ quyền dữ liệu trong điện toán đám mây

2.1. Quyền tài phán trong chuỗi xử lý dữ liệu

Trong môi trường đám mây, doanh nghiệp Việt Nam có thể ký hợp đồng với pháp nhân tại Singapore, dùng nền tảng của tập đoàn Hoa Kỳ và lưu dữ liệu tại nhiều trung tâm. Vị trí lưu trữ chỉ là một yếu tố trong chuỗi kiểm soát, gồm: quyền sở hữu hạ tầng, quyền quản trị tài khoản, quyền nắm giữ khóa mã hóa, quyền quyết định mục đích xử lý, quyền chuyển cho nhà thầu phụ và quyền yêu cầu cung cấp dữ liệu của cơ quan công quyền.

Xung đột phát sinh khi nhiều quốc gia cùng có căn cứ điều chỉnh. Quốc gia nơi đặt máy chủ có thể yêu cầu bảo mật; nước nơi nhà cung cấp đặt trụ sở có thể buộc giao nộp dữ liệu; còn quốc gia nơi chủ thể dữ liệu cư trú lại trao quyền phản đối chuyển dữ liệu. Một tiêu chí lãnh thổ duy nhất không thể xử lý đầy đủ tình huống này. Pháp luật cần xem xét mối liên hệ thực chất của hoạt động xử lý, lợi ích bị ảnh hưởng và khả năng phối hợp quốc tế. Vì vậy, phạm vi áp dụng ngoài lãnh thổ, đánh giá tác động chuyển dữ liệu và tương trợ tư pháp ngày càng quan trọng (Svantesson, 2017).

2.2. Các lớp cấu thành của chủ quyền dữ liệu

Chủ quyền dữ liệu gồm 3 lớp. Chủ quyền pháp lý là khả năng đặt ra và thực thi quy tắc về thu thập, sử dụng, lưu trữ, chuyển giao và xóa dữ liệu; đồng thời buộc nhà cung cấp minh bạch và chấp nhận kiểm toán. Chủ quyền kỹ thuật là khả năng duy trì bảo mật, toàn vẹn, sẵn sàng và phục hồi thông qua mã hóa, quản lý khóa, nhật ký truy cập, sao lưu độc lập và chuyển đổi nhà cung cấp. Chủ quyền của chủ thể dữ liệu thể hiện ở quyền được biết, truy cập, chỉnh sửa, xóa, phản đối và chuyển dữ liệu. Chính sách nhân danh chủ quyền quốc gia nhưng thiếu trách nhiệm giải trình hoặc làm suy giảm quyền riêng tư không phải là mô hình cân bằng (Floridi, 2020).

Bản địa hóa dữ liệu là nghĩa vụ lưu trữ hoặc xử lý trong một lãnh thổ; cư trú dữ liệu mô tả vị trí vật lý; quyền riêng tư điều chỉnh tính hợp pháp và minh bạch của xử lý dữ liệu cá nhân. Bản địa hóa có thể hỗ trợ thực thi pháp luật nhưng không tự động ngăn truy cập từ xa, rò rỉ nội bộ hoặc mệnh lệnh từ nước

nơi nhà cung cấp đặt trụ sở. Vì vậy, chủ quyền phải được đánh giá bằng khả năng kiểm soát, kiểm toán, khôi phục và thực thi, không chỉ bằng tọa độ máy chủ.

3. Kinh nghiệm quốc tế

3.1. Liên minh châu Âu: quyền cơ bản và trách nhiệm giải trình

Liên minh châu Âu xây dựng chủ quyền dữ liệu trên nền tảng bảo vệ quyền cơ bản. GDPR áp dụng cả với một số tổ chức ngoài EU khi cung cấp hàng hóa, dịch vụ hoặc theo dõi hành vi cá nhân tại EU. Văn bản quy định giới hạn mục đích, tối thiểu hóa dữ liệu, giới hạn lưu trữ, bảo mật, trách nhiệm giải trình và các quyền tiếp cận, xóa, phản đối, di chuyển dữ liệu (European Parliament & Council of the European Union, 2016).

Chuyển dữ liệu ra ngoài EU dựa trên quyết định công nhận mức bảo vệ tương đương, điều khoản hợp đồng mẫu, quy tắc nội bộ hoặc ngoại lệ cụ thể. Hoạt động rủi ro cao phải đánh giá tác động, kể cả rủi ro từ nhà xử lý phụ, truy cập từ xa và pháp luật nước thứ ba.

Data Act bổ sung quyền tiếp cận dữ liệu, hạn chế điều khoản bất công, tăng khả năng chuyển đổi dịch vụ và yêu cầu nhà cung cấp chống việc cơ quan nước thứ ba tiếp cận dữ liệu phi cá nhân trái pháp luật EU (European Parliament & Council of the European Union, 2023). EU vì thế coi chống "khóa chặt" công nghệ là thành phần của chủ quyền. Hạn chế là chi phí tuân thủ và đánh giá pháp luật nước thứ ba còn phức tạp.

3.2. Kinh nghiệm từ Trung Quốc: An ninh quốc gia và phân loại dữ liệu

Trung Quốc tiếp cận chủ quyền dữ liệu từ yêu cầu an ninh quốc gia và kiểm soát hạ tầng. Luật An ninh mạng, Luật An ninh dữ liệu và Luật Bảo vệ thông tin cá nhân tạo thành 3 trụ cột. Một số chủ thể, đặc biệt là nhà vận hành hạ tầng thông tin quan trọng và tổ chức xử lý lượng lớn thông tin cá nhân, phải lưu trữ dữ liệu trong nước; chuyển ra nước ngoài có thể phải đánh giá an ninh, chứng nhận hoặc ký hợp đồng tiêu chuẩn. Pháp luật cũng hạn chế việc cung cấp dữ liệu tại Trung Quốc cho cơ quan tư pháp hoặc thực thi pháp luật nước ngoài khi chưa được chấp thuận (National People's Congress of China, 2021).

Quy định về quản lý an ninh dữ liệu mạng có hiệu lực từ năm 2025 cụ thể hóa phân loại dữ liệu, nghĩa vụ của bên xử lý dữ liệu quan trọng và điều kiện chuyển dữ liệu (State Council of the People's Republic of China, 2024). Ưu điểm là tập trung nguồn lực vào dữ liệu có khả năng ảnh hưởng lớn đến an ninh và lợi ích công cộng. Tuy nhiên, nếu tiêu chí dữ liệu quan trọng hoặc cốt lõi không rõ, nghĩa vụ lưu trữ và đánh giá an ninh sẽ tạo bất định, tăng chi phí và giảm linh hoạt. Bài học kinh nghiệm cho Việt Nam là phân loại phải dựa trên hậu quả đo lường được, được công bố minh bạch và rà soát định kỳ.

3.3. Kinh nghiệm từ Hoa Kỳ: Quyền kiểm soát của nhà cung cấp và tiếp cận chứng cứ

Hoa Kỳ không có đạo luật liên bang thống nhất tương đương GDPR mà điều chỉnh theo lĩnh vực và bang. Đối với dữ liệu đám mây, Đạo luật CLOUD năm 2018 khẳng định nhà cung cấp thuộc thẩm quyền Hoa Kỳ có thể bị yêu cầu cung cấp dữ liệu nằm trong quyền chiếm hữu, quản lý hoặc kiểm soát, không phụ thuộc hoàn toàn vào nơi lưu trữ. Hoa Kỳ cũng có thể ký thỏa thuận hành pháp với quốc gia đáp ứng điều kiện nhất định để tiếp cận chứng cứ điện tử nhanh hơn (United States Congress, 2018; U.S. Department of Justice, 2023).

Cách tiếp cận này phản ánh thực tế nhà cung cấp có thể truy xuất dữ liệu xuyên biên giới, nhưng tạo nguy cơ xung đột khi lệnh của Hoa Kỳ yêu cầu giao dữ liệu trong khi pháp luật nước khác cấm chuyển.

Bài học là cam kết dữ liệu đặt tại Việt Nam chưa đủ nếu công ty mẹ hoặc nhân sự toàn cầu vẫn có quyền quản trị, giải mã và trích xuất. Pháp luật Việt Nam cần nhận diện "quyền kiểm soát thực tế" của nhà cung cấp, yêu cầu dữ liệu cho cơ quan nước ngoài được xử lý qua tương trợ tư pháp hoặc kênh được pháp luật công nhận.

4. Thực trạng pháp luật Việt Nam về chủ quyền dữ liệu số trong môi trường điện toán đám mây

4.1. Các nền tảng pháp lý mới

Luật Dữ liệu 60/2024/QH15, có hiệu lực từ ngày 01/7/2025, xác lập dữ liệu quan trọng, dữ liệu cốt lõi và các quy tắc quản trị, bảo vệ, mã hóa, đánh giá rủi ro, xử lý dữ liệu xuyên biên giới. Điều 23 coi việc sử dụng nền tảng đặt ngoài Việt Nam để xử lý dữ liệu là một dạng chuyển, xử lý xuyên biên giới, qua đó tập trung vào hoạt động thay vì chỉ hành vi chuyển tệp (Quốc hội, 2024).

Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, có hiệu lực từ ngày 01/01/2026, quy định về sự đồng ý, quyền của chủ thể, trách nhiệm của bên kiểm soát và xử lý, thông báo vi phạm trong 72 giờ, đánh giá tác động xử lý và chuyển dữ liệu xuyên biên giới. Điều 20 bao gồm cả việc dùng nền tảng ngoài Việt Nam để xử lý dữ liệu thu thập tại Việt Nam (Quốc hội, 2025b).

Luật An ninh mạng số 116/2025/QH15, có hiệu lực từ ngày 01/7/2026, tích hợp an ninh dữ liệu vào bảo vệ an ninh mạng và khẳng định quyền tài phán đối với hoạt động liên quan đến lợi ích quốc gia, trật tự và quyền hợp pháp của tổ chức, cá nhân (Quốc hội, 2025a). Luật Giao dịch điện tử số 20/2023/QH15 công nhận giá trị pháp lý của thông điệp dữ liệu, hợp đồng và nhật ký điện tử (Quốc hội, 2023). Việt Nam vì vậy đã có nền tảng về phân loại, đánh giá rủi ro, chuyển xuyên biên giới, an ninh mạng và quyền cá nhân.

4.2. Những khoảng trống cần khắc phục

Thứ nhất, chưa có chế định thống nhất về dịch vụ điện toán đám mây. Nghĩa vụ nằm rải rác trong nhiều luật và quy định chuyên ngành. Doanh nghiệp phải tự xác định một hoạt động có đồng thời thuộc nhiều thủ tục đánh giá, trong khi cơ quan đầu mối và cơ chế phối hợp hồ sơ chưa rõ.

Thứ hai, tiêu chí dữ liệu quan trọng và dữ liệu cốt lõi cần được cụ thể hóa theo ngành, quy mô, mức độ tập trung, khả năng thay thế và hậu quả khi bị lộ, sửa đổi hoặc gián đoạn. Danh mục quá rộng làm tăng chi phí; danh mục quá hẹp lại bỏ sót tập dữ liệu tổng hợp có rủi ro lớn.

Thứ ba, pháp luật chưa chú trọng đầy đủ đến tài khoản quản trị đặc quyền, khóa mã hóa, chuỗi nhà thầu phụ và khả năng chuyển đổi nhà cung cấp. Rủi ro chủ quyền thường nằm ở "mặt phẳng điều khiển", nơi công ty mẹ hoặc nhân sự nước ngoài có thể truy cập, cấu hình hay đình chỉ dịch vụ. Dữ liệu đặt trong nước chưa đồng nghĩa với quyền kiểm soát trong nước.

Thứ tư, cơ chế xử lý lệnh cung cấp dữ liệu của cơ quan nước ngoài cần chi tiết hơn. Cần quy định nghĩa vụ thông báo, thời hạn phản hồi, bảo toàn chứng cứ, quyền tạm hoãn và trách nhiệm khi hai hệ thống pháp luật đưa ra mệnh lệnh trái ngược. Quyền truy cập, sửa, xóa hoặc phản đối của cá nhân cũng phải gắn với kênh khiếu nại và cơ chế xác định trách nhiệm trong chuỗi xử lý.

5. Một số kiến nghị hoàn thiện pháp luật của Việt Nam về chủ quyền dữ liệu số trong môi trường điện toán đám mây

Một là, ban hành nghị định hoặc chương chuyên biệt về điện toán đám mây, thống nhất khái niệm nhà

cung cấp, nhà xử lý phụ, vùng dữ liệu, truy cập từ xa và chuyển đổi dịch vụ. Cần áp dụng cơ chế "một hồ sơ - nhiều mục đích", xác định cơ quan đầu mối và tránh kiểm tra trùng lặp.

Hai là, áp dụng bản địa hóa theo rủi ro. Dữ liệu cốt lõi liên quan trực tiếp đến quốc phòng, an ninh hoặc hạ tầng thiết yếu có thể chịu mức kiểm soát cao. Dữ liệu quan trọng được chuyển ra nước ngoài khi có đánh giá tác động, mã hóa, kiểm soát khóa và kế hoạch khôi phục. Dữ liệu thông thường nên được lưu chuyển trên cơ sở tuân thủ quyền riêng tư, an ninh và hợp đồng (Casalini & López González, 2019).

Ba là, chuyển trọng tâm từ vị trí máy chủ sang kiểm soát có thể kiểm chứng. Hợp đồng đám mây đối với dữ liệu quan trọng phải quy định bản đồ luồng dữ liệu, nhà thầu phụ, tài khoản đặc quyền, kiểm soát khóa mã hóa, nhật ký truy cập, kiểm toán độc lập, thông báo yêu cầu của cơ quan nước ngoài, hoàn trả và xóa dữ liệu, định dạng xuất dữ liệu, hỗ trợ chuyển đổi và trách nhiệm khi gián đoạn. Khu vực công cần tích hợp các yêu cầu này vào đấu thầu và nghiệm thu.

Bốn là, thiết lập cơ chế đánh giá xung đột pháp luật. Trước khi dùng dịch vụ nước ngoài cho dữ liệu nhạy cảm, tổ chức phải đánh giá pháp luật nơi nhà cung cấp hoặc công ty mẹ đặt trụ sở. Nhà cung cấp phải thông báo trước khi giao dữ liệu cho cơ quan nước ngoài, trừ trường hợp bị cấm trên cơ sở pháp lý rõ ràng. Việt Nam cần mở rộng tương trợ tư pháp và thỏa thuận về chứng cứ điện tử.

Năm là, tăng cường quyền cá nhân, giám sát độc lập và tự chủ hạ tầng. Cổng thông tin bảo vệ dữ liệu cá nhân cần hỗ trợ yêu cầu, khiếu nại và theo dõi tiến độ; cơ quan giám sát phải có năng lực kiểm tra kỹ thuật và yêu cầu khắc phục. Việt Nam cần phát triển trung tâm dữ liệu, dịch vụ đám mây an toàn, tiêu chuẩn mở và quản lý khóa trong nước; nhưng "đám mây có chủ quyền" phải bảo đảm quyền lựa chọn, chuyển đổi, kiểm toán và phục hồi, không đồng nghĩa với loại bỏ nhà cung cấp nước ngoài.

6. Kết luận

Điện toán đám mây làm cho chủ quyền dữ liệu trở thành vấn đề kiểm soát đa tầng, không còn là quan hệ đơn giản giữa dữ liệu và lãnh thổ. EU nhấn mạnh quyền cơ bản và trách nhiệm giải trình; Trung Quốc ưu tiên an ninh quốc gia, phân loại và kiểm soát chuyển dữ liệu; Hoa Kỳ dựa nhiều vào quyền kiểm soát của nhà cung cấp và tiếp cận chứng cứ. Mỗi mô hình có ưu điểm, nhưng đồng thời tạo chi phí tuân thủ hoặc rủi ro xung đột quyền tài phán.

Việt Nam đã có nền tảng pháp lý quan trọng, nhưng cần chuyển từ nguyên tắc chung sang cơ chế thực thi thống nhất cho dịch vụ đám mây. Trọng tâm phải là quản trị theo rủi ro, kiểm soát kỹ thuật có thể chứng minh, quyền của chủ thể dữ liệu, khả năng chuyển đổi nhà cung cấp và cơ chế xử lý yêu cầu xuyên biên giới. Chỉ khi kết hợp năng lực pháp lý, hạ tầng kỹ thuật và trách nhiệm giải trình, chủ quyền dữ liệu mới đồng thời hỗ trợ an ninh quốc gia, quyền con người và phát triển kinh tế số ■

TÀI LIỆU THAM KHẢO:

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

Quốc hội. (2024). Luật số 60/2024/QH15: Luật Dữ liệu, ban hành ngày 30/11/2024.

Quốc hội. (2025a). Luật số 16/2025/QH15: Luật An ninh mạng, ban hành ngày 10/12/2025.

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

Casalini, F., & López González, J. (2019). Trade and cross-border data flows (OECD Trade Policy Papers No. 220). OECD Publishing. https://doi.org/10.1787/b2023a47-en

Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305-2322. https://doi.org/10.1177/1461444819865984

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, L 2023/2854. https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

National People's Congress of China. (2021). Personal Information Protection Law of the People's Republic of China. https://en.spp.gov.cn/2021-12/29/c_948419_2.htm

State Council of the People's Republic of China. (2024). Regulations on Network Data Security Management (Decree No. 790). https://english.www.gov.cn/

Svantesson, D. J. B. (2017). Solving the Internet jurisdiction puzzle. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

United States Congress. (2018). Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213. https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf

U.S. Department of Justice. (2023). Regarding CLOUD Act executive agreements. https://www.justice.gov/criminal/criminal-oia/regarding-cloud-act-executive-agreements