

MÔ HÌNH TRÁCH NHIỆM CHIA SẺ TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN ĐIỆN TOÁN Đám Mây: KINH NGHIỆM QUỐC TẾ VÀ GỢI MỞ CHO VIỆT NAM

HOÀNG VĂN THIÊN
Khoa Luật, Học viện Phụ nữ Việt Nam

Nhận bài ngày 16/9/2026. Sửa chữa xong 12/10/2026. Duyệt đăng 16/10/2026.

Abstract

This article examines the theoretical foundations of the shared responsibility model for personal data protection in cloud computing environments. Drawing on a comparative analysis of relevant legislation and regulatory approaches in the European Union, the United States, and Singapore, it assesses Vietnam's existing legal framework and identifies regulatory gaps in the allocation of responsibilities among cloud service stakeholders. Based on these findings, the article proposes recommendations for improving Vietnamese law in a manner that reflects the distinctive technical and operational characteristics of cloud computing.

Keywords: Cloud computing, personal data protection, shared responsibility.

1. Đặt vấn đề

Điện toán đám mây là tài nguyên dùng chung, hạ tầng được trừu tượng hóa, dữ liệu được lưu trữ và xử lý xuyên biên giới qua nhiều nhà cung cấp, khiến cho việc bảo vệ dữ liệu cá nhân của khách hàng không còn nằm hoàn toàn trong tay một chủ thể duy nhất, mà có sự tham gia của nhiều chủ thể khác nhau (Hon et al., 2012). Khi dữ liệu cá nhân được lưu trữ và xử lý phân tán trên các nền tảng đám mây, tổ chức thu thập dữ liệu không còn trực tiếp nắm giữ hay toàn quyền kiểm soát dữ liệu được lưu giữ.

Sự phân tách giữa quyền kiểm soát đối với mục đích xử lý và quyền kiểm soát kỹ thuật đối với hạ tầng lưu trữ đã tạo ra một khoảng trống pháp lý. Cụ thể, khi dữ liệu cá nhân bị xâm phạm, rò rỉ hoặc xử lý trái phép trong môi trường điện toán đám mây, chủ thể nào phải chịu trách nhiệm pháp lý (TNPL) và phạm vi nghĩa vụ của mỗi bên được phân định ra sao? Để giải quyết bài toán phân định TNPL trong một môi trường mang tính phụ thuộc lẫn nhau về công nghệ, mô hình trách nhiệm chia sẻ đã ra đời.

Ở phạm vi quốc tế, Liên minh châu Âu, Hoa Kỳ và Singapore đã xây dựng khung pháp lý khác nhau về trách nhiệm bảo vệ dữ liệu cá nhân (BVDLCN) trên điện toán đám mây, nhằm bảo vệ quyền lợi của cá nhân, tổ chức và doanh nghiệp trên không gian mạng. Ngoài ba hệ thống nêu trên, một số quốc gia châu Á khác cũng đã ban hành luật chuyên biệt về điện toán đám mây, tiêu biểu là Hàn Quốc với Đạo luật về phát triển điện toán đám mây và bảo vệ người dùng.

Tại Việt Nam, nhà nước đã ban hành một số văn bản quy phạm pháp luật như Luật Bảo vệ dữ liệu cá nhân 2025, 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 dữ liệu cá nhân (LBVDLCN), cùng Luật An ninh mạng năm 2025. Tuy nhiên, hệ thống pháp luật hiện hành vẫn còn nhiều khoảng trống và bất cập khi chưa làm rõ được cơ chế phân định trách nhiệm giữa các chủ thể khi tham gia quan hệ cung cấp dịch vụ điện toán đám mây.

Bài viết đối chiếu với kinh nghiệm lập pháp của một số quốc gia và khu vực trên thế giới để rút ra hàm ý chính sách phù hợp cho pháp luật Việt Nam. Kết quả nghiên cứu vừa có ý nghĩa góp phần hoàn

Email: thienhv@hvpnvvn.edu.vn

thiện hệ thống pháp luật, vừa nâng cao hiệu quả thực thi pháp luật trên thực tế, hướng tới mục tiêu phát triển bền vững nền kinh tế số của Việt Nam trong giai đoạn hiện nay.

2. Nội dung nghiên cứu

2.1. Khái quát chung về mô hình trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây

Dù có nhiều định nghĩa khác nhau, về cơ bản có thể hiểu điện toán đám mây là mô hình cung cấp từ xa các tài nguyên công nghệ thông tin như máy chủ, không gian lưu trữ, cơ sở dữ liệu, phần mềm qua môi trường Internet. Thay vì lưu giữ dữ liệu và phần mềm cố định trên thiết bị lưu trữ cá nhân vốn bị giới hạn về khả năng tiếp cận và tính di động, người dùng có thể truy cập dữ liệu của mình mọi lúc, mọi nơi, trong khi doanh nghiệp và cá nhân không còn phải tự đầu tư, vận hành và bảo trì hệ thống phần cứng phức tạp, qua đó tối ưu hóa chi phí hạ tầng công nghệ thông tin.

Mô hình trách nhiệm chia sẻ bắt nguồn từ thực tiễn quản trị an toàn thông tin của chính các nhà cung cấp dịch vụ đám mây lớn như Amazon Web Services, Microsoft Azure và Google Cloud, vốn sử dụng mô hình này như một công cụ để phân định ranh giới nghĩa vụ bảo mật trong hợp đồng cung cấp dịch vụ với khách hàng (Amazon Web Services, n.d.-a). Dưới góc độ pháp lý, đây là một thỏa thuận có tính chất ràng buộc các bên trong quan hệ hợp đồng và không có giá trị đối kháng với chủ thể dữ liệu hay cơ quan quản lý nhà nước. Mô hình trách nhiệm chia sẻ không tạo ra một chế định pháp lý mới, mà vận dụng nguyên tắc kiểm soát thực tế, vốn là tiêu chí xác định vai trò bên kiểm soát/bên xử lý trong pháp luật BVDLCN vào bối cảnh kỹ thuật đặc thù của điện toán đám mây, nơi việc kiểm soát bị phân tầng theo chiều dọc thay vì tập trung vào một chủ thể duy nhất như trong mô hình quản trị công nghệ thông tin truyền thống. Do đó, đây được xem là cơ sở để mô hình trách nhiệm chia sẻ có giá trị quy phạm, chứ không chỉ là công cụ quản trị nội bộ của ngành công nghiệp đám mây (Kamarinou et al., 2021).

Có thể định nghĩa mô hình trách nhiệm chia sẻ trong BVDLCN trên điện toán đám mây là tổng hợp các quy phạm pháp luật xác định trách nhiệm tuân thủ cũng như trách nhiệm bồi thường thiệt hại giữa nhà cung cấp dịch vụ điện toán đám mây và khách hàng sử dụng dịch vụ, dựa trên mức độ kiểm soát kỹ thuật thực tế của mỗi chủ thể, TNPL của những chủ thể trong điện toán đám mây không còn mang tính độc lập mà trở thành một mạng lưới trách nhiệm đa tầng. Từ khái niệm trên, mô hình này có ba đặc trưng cơ bản như sau:

Thứ nhất, tính tương đối và linh hoạt theo mô hình dịch vụ. Phạm vi trách nhiệm của khách hàng tăng dần theo thứ tự SaaS → PaaS → IaaS, do mức độ kiểm soát kỹ thuật của khách hàng đối với hệ thống cũng tăng dần theo thứ tự đó (Amazon Web Services, n.d.-a).

Thứ hai, tính không thể chuyển giao trách nhiệm. Dù nhà cung cấp dịch vụ có thể đóng vai trò là bên xử lý dữ liệu và phải tuân thủ các nghĩa vụ kỹ thuật, khách hàng hoặc bên kiểm soát dữ liệu vẫn luôn là chủ thể chịu TNPL trước chủ thể dữ liệu và trước cơ quan quản lý nhà nước về việc dữ liệu được xử lý hợp pháp (Amazon Web Services, n.d.-a).

Thứ ba, tính đa tầng trong chuỗi cung ứng. Một dịch vụ đám mây thường không chỉ có hai chủ thể mà có thể bao gồm nhiều bên xử lý thứ cấp như nhà cung cấp hạ tầng mạng, nhà cung cấp phần mềm hỗ trợ, đòi hỏi trách nhiệm phải được truyền theo chuỗi hợp đồng để bảo đảm tính liên tục của việc bảo vệ dữ liệu (Trần Quỳnh Anh & Chu Thị Thu Hà, 2026).

2.2. Pháp luật một số quốc gia và khu vực về mô hình trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây

2.2.1. Pháp luật Liên minh châu Âu

Quy định bảo vệ dữ liệu chung (General Data Protection Regulation - GDPR) bao quát các mối quan hệ phức tạp trong môi trường đám mây thông qua việc định danh hai nhóm chủ thể: bên kiểm soát dữ liệu và bên xử lý dữ liệu (Quy định [EU] 2016/679, 2016, Điều 4(7)-4(8)). Bên kiểm soát và bên xử lý phải ký kết hợp đồng, trong đó quy định cụ thể về đối tượng, thời hạn, tính chất, mục đích xử lý, loại dữ liệu

cá nhân, nhóm chủ thể dữ liệu cũng như quyền và nghĩa vụ của bên kiểm soát. Bên xử lý chỉ được xử lý dữ liệu theo hướng dẫn của bên kiểm soát, các nhân sự được phép xử lý dữ liệu phải cam kết bảo mật đồng thời áp dụng các biện pháp an ninh theo Điều 32 GDPR. Đặc biệt, không được thuê bên xử lý thứ cấp nếu không có sự chấp thuận trước bằng văn bản của bên kiểm soát. Trường hợp bên xử lý thứ cấp không thực hiện đúng các nghĩa vụ bảo vệ dữ liệu, bên xử lý ban đầu vẫn phải chịu trách nhiệm đầy đủ trước bên kiểm soát đối với việc thực hiện nghĩa vụ của bên xử lý thứ cấp đó.

Theo Điều 4(7) GDPR, bên kiểm soát dữ liệu là chủ thể quyết định mục đích và phương tiện xử lý dữ liệu. Trong môi trường đám mây, các doanh nghiệp hoặc cơ quan, tổ chức thuê dịch vụ đám mây để quản trị thông tin khách hàng, nhân sự đều giữ vai trò bên kiểm soát dữ liệu. Đây là chủ thể chịu trách nhiệm trước pháp luật và trước chủ thể dữ liệu về tính hợp pháp của hoạt động xử lý. Việc thuê dịch vụ đám mây không đồng nghĩa với việc chuyển giao TNPL này cho nhà cung cấp dịch vụ (European Data Protection Supervisor, 2018).

Trong khi đó, theo Điều 4(8) GDPR, bên xử lý dữ liệu là chủ thể thực hiện việc xử lý dữ liệu, thường là các nhà cung cấp dịch vụ đám mây (CSP). Tuy nhiên, Điều 28 và Điều 32 GDPR đặt ra một loạt nghĩa vụ trực tiếp cho bên xử lý dữ liệu, bao gồm việc áp dụng các biện pháp kỹ thuật phù hợp để bảo đảm an toàn dữ liệu, hỗ trợ bên kiểm soát dữ liệu thực hiện quyền của chủ thể dữ liệu và thông báo kịp thời khi phát hiện sự cố rò rỉ dữ liệu.

Về trách nhiệm bồi thường thiệt hại, theo Điều 82(2), bên kiểm soát chịu trách nhiệm về mọi thiệt hại phát sinh từ hoạt động xử lý vi phạm GDPR và chỉ được miễn trừ trách nhiệm nếu chứng minh được mình hoàn toàn không liên quan đến sự kiện gây thiệt hại (Điều 82(3)). Trong khi đó, trách nhiệm của bên xử lý phát sinh khi không tuân thủ nghĩa vụ riêng mà GDPR đặt ra cho bên xử lý, hoặc thực hiện trái với hướng dẫn của bên kiểm soát. Khi phát sinh trách nhiệm, Điều 82(4)-(5) quy định cơ chế trách nhiệm liên đới, theo đó mỗi bên chịu trách nhiệm trước chủ thể dữ liệu, sau đó mới xác định trách nhiệm của mỗi bên theo mức độ lỗi tương ứng.

Ngoài GDPR, EU còn ban hành Luật Dữ liệu (EU Data Act), có hiệu lực chính thức từ tháng 9/2025, trong đó dành một phần quy định riêng về hợp đồng dịch vụ điện toán đám mây, hướng tới mục tiêu thúc đẩy khả năng chuyển đổi nhà cung cấp dịch vụ đám mây. Quy định này cho thấy EU đang tiếp cận theo hướng bổ sung hợp đồng mẫu, bên cạnh khung pháp luật là GDPR và Data Act để hỗ trợ thực thi mô hình trách nhiệm chia sẻ trong thực tiễn hợp đồng dịch vụ đám mây.

2.2.2. Pháp luật Hoa Kỳ

Hoa Kỳ không có một luật liên bang thống nhất về BVDLCN theo mô hình toàn diện như Liên minh châu Âu, mà phát triển theo mô hình pháp luật phân mảnh giữa các tiểu bang. Trong số đó, Đạo luật quyền riêng tư California (California Privacy Rights Act - CPRA) đã tạo ra mức độ ảnh hưởng tương đương GDPR của Liên minh Châu Âu trong phạm vi Hoa Kỳ. Đạo luật này phân chia các chủ thể tham gia xử lý dữ liệu bao gồm bên kiểm soát dữ liệu và bên xử lý dữ liệu (California Privacy Rights Act, 2020/2023).

Điểm đặc trưng của pháp luật Hoa Kỳ khi áp dụng vào môi trường điện toán đám mây là cơ chế kiểm soát hành vi bán hoặc chia sẻ dữ liệu trái phép. CPRA quy định rằng việc bên kiểm soát chuyển dữ liệu lên hệ thống đám mây chỉ được coi là hợp pháp khi hợp đồng quy định CSP không được giữ lại, sử dụng hoặc tiết lộ dữ liệu cá nhân đó cho bất kỳ mục đích nào khác ngoài phạm vi cung cấp dịch vụ kỹ thuật (California Privacy Rights Act, 2020/2023, § 1798.140(ag), (ad)). Nếu thiếu các quy định này trong hợp đồng, việc lưu trữ dữ liệu trên đám mây có thể bị coi là hành vi bán hoặc chia sẻ dữ liệu trái phép cho bên thứ ba, và có thể phải chịu các chế tài dân sự nghiêm khắc từ Cơ quan bảo vệ quyền riêng tư California (CPPA).

Bên cạnh các quy định pháp luật, Hoa Kỳ kiểm soát rủi ro trên môi trường đám mây thông qua hệ thống tiêu chuẩn kỹ thuật. NIST đã ban hành khung an ninh mạng cùng các hướng dẫn chuyên biệt về điện toán đám mây (National Institute of Standards and Technology, 2018). Các tiêu chuẩn này chỉ rõ rằng trách nhiệm chia sẻ không cố định, mà thay đổi liên tục dựa trên kiến trúc hệ thống và loại hình dịch vụ được triển khai. Đóng góp quan trọng của tiêu chuẩn NIST đối với khoa học pháp lý là cung

cấp một bộ công cụ kỹ thuật giúp các cơ quan tài phán và các bên tham gia hợp đồng xác định mức độ kiểm soát thực tế của từng chủ thể. Nếu một sự cố xảy ra ở lớp hạ tầng mà CSP tuyên bố đã bảo mật nhưng không chứng minh được bằng các chứng nhận kiểm toán phù hợp, CSP có thể phải chịu trách nhiệm về lỗi của mình (National Institute of Standards and Technology, 2011).

Đối với khu vực công, Hoa Kỳ còn vận hành Chương trình quản lý rủi ro và cấp phép liên bang (Federal Risk and Authorization Management Program - FedRAMP), một cơ chế chuẩn hóa việc đánh giá bảo mật, cấp phép và giám sát liên tục đối với các sản phẩm, dịch vụ điện toán đám mây mà cơ quan liên bang sử dụng (General Services Administration, n.d.). FedRAMP xây dựng ma trận trách nhiệm bảo mật, phân định cụ thể trách nhiệm của CSP và của cơ quan sử dụng dịch vụ theo từng nhóm biện pháp kiểm soát an ninh, tương ứng với từng mô hình dịch vụ đám mây.

2.2.3. Pháp luật Singapore

Singapore là một ví dụ điển hình cho mô hình lập pháp cân bằng giữa bảo vệ quyền con người và thúc đẩy nền kinh tế số tại châu Á. Đạo luật bảo vệ dữ liệu cá nhân năm 2012 Singapore (Personal Data Protection Act - PDPA) thiết lập cơ chế quản trị trách nhiệm dựa trên nghĩa vụ của tổ chức kiểm soát dữ liệu và bên trung gian dữ liệu, tương ứng với vai trò của bên xử lý dữ liệu (Personal Data Protection Act, 2012).

Cách tiếp cận của Singapore mang tính thực tiễn cao khi quy định rằng tổ chức thuê dịch vụ đám mây vẫn phải chịu trách nhiệm trước pháp luật về việc bảo đảm an toàn dữ liệu, ngay cả khi toàn bộ dữ liệu đã được giao cho một CSP xử lý (Personal Data Protection Act, 2012). Tuy nhiên, để bảo vệ các doanh nghiệp trong nước trước các CSP đa quốc gia có quy mô lớn, cơ quan quản lý phát triển truyền thông và thông tin và Ủy ban BVDLCN của Singapore đã ban hành các hướng dẫn chuyên ngành về điện toán đám mây. Các hướng dẫn này yêu cầu tổ chức phải thực hiện quy trình thẩm định trước khi ký hợp đồng, bao gồm việc đánh giá năng lực bảo mật, vị trí địa lý của máy chủ lưu trữ và khả năng thực hiện quyền kiểm toán của doanh nghiệp đối với hệ thống của CSP (Personal Data Protection Commission Singapore, 2021).

2.3. Bài học kinh nghiệm cho Việt Nam

Từ việc phân tích quy định pháp luật của Liên minh châu Âu, Hoa Kỳ và Singapore, có thể rút ra một số bài học kinh nghiệm cho Việt Nam như sau:

Thứ nhất, trách nhiệm chia sẻ không đồng nghĩa với chia đều trách nhiệm. TNPL cần đi đôi với quyền kiểm soát kỹ thuật thực tế và khả năng phòng ngừa rủi ro tại thời điểm xảy ra sự cố, như cách GDPR và PDPA đều giới hạn phạm vi trách nhiệm trực tiếp của bên xử lý/bên trung gian theo phạm vi kiểm soát thực tế của họ.

Thứ hai, đề cao vai trò của hợp đồng mẫu xử lý dữ liệu (DPA). Hợp đồng xử lý dữ liệu không thể chỉ là sự thỏa thuận thương mại tự do, dễ bị áp đặt bởi các CSP có vị thế thị trường lớn.

Thứ ba, cần ghi nhận các nghĩa vụ trực tiếp của CSP mang tính công quyền, như nghĩa vụ báo cáo sự cố trong khoảng thời gian xác định (thông lệ quốc tế phổ biến là 72 giờ theo GDPR, hoặc theo cơ chế đánh giá khẩn trương như Điều 26C-26D PDPA) và nghĩa vụ hợp tác với cơ quan điều tra, chứ không chỉ dừng lại ở các cam kết chất lượng dịch vụ (SLA) mang tính thương mại.

Thứ tư, cần kết hợp hài hòa giữa pháp luật và tiêu chuẩn kỹ thuật, theo kinh nghiệm của Hoa Kỳ (NIST). Việc nội hóa các tiêu chuẩn quốc tế (như chuỗi tiêu chuẩn ISO/IEC 27000) vào văn bản quy phạm pháp luật là giải pháp phù hợp đối với lĩnh vực công nghệ có tốc độ biến đổi nhanh.

2.4. Pháp luật Việt Nam về trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây

2.4.1. Quy định của pháp luật về trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây

Đối với trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây, khoản 1 Điều 37 Luật bảo vệ dữ liệu cá nhân 2025 quy định: bên kiểm soát dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu cá nhân về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra. Bên kiểm soát dữ liệu, với

tư cách là chủ thể quyết định mục đích và phương tiện xử lý phải chịu trách nhiệm đối với mọi hậu quả phát sinh, kể cả trong trường hợp việc xử lý được thực hiện thông qua bên xử lý dữ liệu hoặc bên thứ ba. Bên kiểm soát dữ liệu là chủ thể nắm giữ quyền quyết định, do đó cũng phải gánh chịu hệ quả pháp lý tương ứng khi việc xử lý gây thiệt hại đến quyền và lợi ích của chủ thể dữ liệu.

Theo điểm d khoản 2 Điều 37 Luật Bảo vệ dữ liệu cá nhân 2025 quy định, bên xử lý dữ liệu cá nhân chịu trách nhiệm trước bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân về thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra. Khoản 2 Điều 12 Nghị định số 356/2025/NĐ-CP quy định các tổ chức, cá nhân ký kết hợp đồng có liên quan tới xử lý dữ liệu cá nhân với các tổ chức cung cấp dịch vụ điện toán đám mây có trách nhiệm xác định rõ luồng xử lý dữ liệu cá nhân, vai trò các bên trong hoạt động cung cấp dịch vụ điện toán đám mây và trách nhiệm tương ứng.

Cơ chế trách nhiệm chia sẻ trên đám mây không chỉ tuân thủ các nguyên tắc của Luật Bảo vệ dữ liệu cá nhân 2025, mặt khác phải đáp ứng các yêu cầu nghiêm ngặt về phòng, chống tấn công mạng, giám sát an ninh và sẵn sàng ứng phó sự cố theo sự điều phối của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an (Bộ Công an, 2025). Đặc tính lưu trữ phân tán xuyên biên giới của điện toán đám mây đặt ra thách thức đáng kể đối với việc thực thi chủ quyền quốc gia trên không gian mạng.

Theo khoản 3 Điều 25 Luật An ninh mạng 2025, các doanh nghiệp nước ngoài cung cấp dịch vụ điện toán đám mây xuyên biên giới, có hoạt động thu thập, phân tích dữ liệu của người dùng Việt Nam, phải lưu trữ dữ liệu này tại hệ thống máy chủ đặt trong lãnh thổ Việt Nam và thiết lập chi nhánh hoặc văn phòng đại diện theo điều kiện luật định (Quốc hội, 2025). Quy định này nhằm bảo đảm quyền kiểm soát của Nhà nước, khẳng định rằng dù công nghệ đám mây mang tính toàn cầu, khi vận hành tại Việt Nam, các CSP đa quốc gia vẫn phải tuân thủ quyền tài phán của pháp luật Việt Nam và không được lấy lý do máy chủ đặt tại nước ngoài để từ chối hợp tác điều tra khi xảy ra sự cố vi phạm pháp luật (Trần Minh Hải, 2026).

Cơ bản, pháp luật Việt Nam đã đạt được những bước tiến đáng kể và dần tiệm cận với các chuẩn mực quốc tế như GDPR hay các tiêu chuẩn của NIST trong việc tiếp cận mô hình trách nhiệm chia sẻ. Cụ thể, việc xác định rõ tư cách bên kiểm soát dữ liệu và bên xử lý dữ liệu giúp cho tòa án và cơ quan quản lý xác định đúng chủ thể chịu trách nhiệm khi xảy ra tranh chấp hoặc sự cố an ninh mạng. Về chế tài, việc nâng mức xử phạt hành chính dựa trên tỷ lệ phần trăm doanh thu, cùng với các hình thức xử lý bổ sung đã tạo ra sức răn đe đáng kể, góp phần thúc đẩy các CSP đầu tư nghiêm túc hơn cho hạ tầng bảo mật khi vận hành tại Việt Nam.

2.4.2. Một số hạn chế, bất cập

Mặc dù đã xây dựng được một nền tảng thể chế tương đối tiến bộ, tuy nhiên pháp luật Việt Nam hiện hành vẫn còn một số hạn chế về trách nhiệm chia sẻ trong BVDLCN trên điện toán đám mây như sau:

Thứ nhất, Việt Nam chưa có văn bản pháp luật riêng biệt quy định về điện toán đám mây, dịch vụ điện toán đám mây hoặc hợp đồng dịch vụ điện toán đám mây. Điều này tạo ra bất cập vì các quy định về bảo vệ dữ liệu cá nhân vẫn chưa thể giải quyết được các vấn đề mang tính đặc thù của quan hệ hợp đồng dịch vụ điện toán đám mây.

Thứ hai, các quy định tại Điều 30 Luật Bảo vệ dữ liệu cá nhân 2025 còn mang tính nguyên tắc, định hướng, chưa cụ thể hóa được sự phân định trách nhiệm tương ứng với từng mô hình dịch vụ như kinh nghiệm của Hoa Kỳ hay thông lệ chung của ngành công nghiệp đám mây.

Thứ ba, quy định về thông báo vi phạm dữ liệu cá nhân tại Điều 23 Luật Bảo vệ dữ liệu cá nhân 2025 chỉ áp dụng đối với trường hợp phát hiện hành vi vi phạm có thể gây tổn hại đến quốc phòng, an ninh quốc gia hoặc xâm phạm tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của chủ thể dữ liệu, mà chưa quy định rõ trách nhiệm thông báo trong trường hợp xảy ra thiệt hại về dữ liệu cá nhân nhưng không xác định được hành vi vi phạm cụ thể.

Thứ tư, pháp luật Việt Nam chưa có cơ chế giám sát chuỗi cung ứng nhiều tầng đối với dịch vụ điện

toán đám mây trong khi đây là đặc trưng phổ biến của dịch vụ đám mây với sự tham gia của nhiều bên xử lý thứ cấp. Điều này dẫn đến khó khăn trong việc xác định chủ thể chịu trách nhiệm khi sự cố xảy ra ở nhà cung cấp thứ cấp mà khách hàng không trực tiếp giao kết hợp đồng.

Thứ năm, pháp luật Việt Nam chưa quy định bộ tiêu chí kỹ thuật, tiêu chuẩn, chứng chỉ bắt buộc về bảo đảm an ninh mạng, an toàn thông tin áp dụng chung cho toàn ngành dịch vụ điện toán đám mây. Hiện nay, Quyết định số 8297/QĐ-BCA-A05 ngày 09/10/2025 của Bộ Công an ban hành bộ tiêu chí đảm bảo an ninh mạng đối với nền tảng điện toán đám mây mới chỉ áp dụng cho các nền tảng phục vụ Chính phủ điện tử, Chính quyền điện tử, và chỉ mang tính khuyến khích tham khảo đối với các cơ quan, tổ chức khác (Bộ Công an, 2025).

Thứ sáu, vấn đề địa điểm đặt máy chủ và lưu trữ dữ liệu chưa được quy định cụ thể trong hợp đồng dịch vụ điện toán đám mây. Phần lớn thị phần dịch vụ đám mây tại Việt Nam do các nhà cung cấp nước ngoài như Amazon Web Services, Google, Microsoft nắm giữ với máy chủ đặt ngoài lãnh thổ Việt Nam, tuy nhiên pháp luật hiện hành chưa yêu cầu hợp đồng dịch vụ điện toán đám mây phải nêu cụ thể địa điểm đặt máy chủ, lưu trữ dữ liệu, cũng như nghĩa vụ thông báo khi có thay đổi địa điểm, gây khó khăn cho việc xác định pháp luật điều chỉnh khi có tranh chấp hoặc khi cần thực thi các biện pháp bảo vệ dữ liệu cá nhân liên quan đến chuyển dữ liệu xuyên biên giới.

2.5. Một số giải pháp hoàn thiện pháp luật Việt Nam

2.5.1. Cần sớm xây dựng và ban hành văn bản pháp luật quy định riêng về điện toán đám mây, dịch vụ điện toán đám mây và hợp đồng dịch vụ điện toán đám mây.

2.5.2. Cần có văn bản hướng dẫn thi hành để cụ thể hóa Điều 30 Luật Bảo vệ dữ liệu cá nhân 2025 về nguyên tắc trách nhiệm chia sẻ theo từng mô hình dịch vụ.

2.5.3. Hoàn thiện quy định về thông báo vi phạm dữ liệu cá nhân theo hướng: 1) Bổ sung trách nhiệm thông báo trong trường hợp xảy ra thiệt hại về dữ liệu cá nhân nhưng không xác định được hành vi vi phạm cụ thể; 2) Bổ sung chủ thể dữ liệu cá nhân vào danh sách đối tượng phải được thông báo và 3) Quy định rõ nghĩa vụ của CSP với tư cách bên trung gian phải thông báo ngay cho khách hàng khi phát hiện hoặc có căn cứ nghi ngờ vi phạm.

2.5.4. Bổ sung quy định về giám sát chuỗi cung ứng nhiều tầng trong dịch vụ điện toán đám mây, cụ thể 1) Nhà cung cấp dịch vụ điện toán đám mây chỉ được thuê bên xử lý thứ cấp khi có sự chấp thuận trước của khách hàng; 2) Nhà cung cấp dịch vụ vẫn phải chịu trách nhiệm đầy đủ trước khách hàng đối với việc thực hiện nghĩa vụ bảo vệ dữ liệu cá nhân của bên xử lý thứ cấp và 3) Bên kiểm soát dữ liệu có trách nhiệm thẩm định năng lực của nhà cung cấp dịch vụ điện toán đám mây trước khi giao kết hợp đồng và phải duy trì việc theo dõi, giám sát trong suốt quá trình cung cấp dịch vụ.

2.5.5. Xây dựng bộ tiêu chí kỹ thuật, tiêu chuẩn, chứng chỉ bảo vệ dữ liệu cá nhân bắt buộc áp dụng cho toàn ngành dịch vụ điện toán đám mây tại Việt Nam, không chỉ giới hạn ở phạm vi phục vụ Chính phủ điện tử, chính quyền điện tử như Quyết định số 8297/QĐ-BCA-A05 hiện hành.

2.5.6. Bổ sung quy định về nội dung mẫu của hợp đồng dịch vụ điện toán đám mây. Việc ban hành các điều khoản mẫu chỉ mang tính tham khảo, sẽ giúp các doanh nghiệp nhỏ và vừa vốn không có đủ năng lực pháp lý, có thể đàm phán hợp đồng với các nhà cung cấp dịch vụ đám mây xuyên quốc gia.

2.5.7. Bổ sung quy định về nghĩa vụ công khai thông tin địa điểm đặt máy chủ, lưu trữ dữ liệu trong hợp đồng dịch vụ điện toán đám mây và nghĩa vụ thông báo khi có thay đổi địa điểm, đặc biệt trong trường hợp dữ liệu được lưu trữ hoặc xử lý ngoài lãnh thổ Việt Nam.

2.5.8. Cần tăng cường năng lực thực thi và giám sát của cơ quan chuyên trách BVDLCN đối với hoạt động cung cấp dịch vụ điện toán đám mây. Đồng thời, cần đẩy mạnh phổ biến kiến thức về an ninh mạng và BVDLCN cho cả doanh nghiệp cung cấp dịch vụ và người sử dụng dịch vụ điện toán đám mây.

3. Kết luận

Pháp luật Việt Nam hiện hành vẫn chưa cụ thể hóa được sự phân định trách nhiệm tương ứng với

từng mô hình dịch vụ đám mây, chưa có cơ chế giám sát chuỗi cung ứng nhiều tầng, chưa có bộ tiêu chuẩn kỹ thuật bắt buộc áp dụng rộng rãi, và còn thiếu khung pháp lý riêng cho hợp đồng dịch vụ điện toán đám mây. Việc tiếp thu có chọn lọc kinh nghiệm quốc tế sẽ giúp Việt Nam xây dựng một khung pháp lý đầy đủ, hiệu quả về trách nhiệm chia sẻ trong bảo vệ dữ liệu cá nhân trên điện toán đám mây, qua đó vừa bảo vệ tốt hơn quyền và lợi ích hợp pháp của chủ thể dữ liệu, vừa tạo môi trường pháp lý minh bạch, thuận lợi để thúc đẩy sự phát triển bền vững của thị trường điện toán đám mây tại Việt Nam trong giai đoạn chuyển đổi số 2025-2030.

Tài liệu tham khảo

- Act on the Development of Cloud Computing and Protection of Its Users. (2015) sửa đổi bổ sung 2021).
- Amazon Web Services. (n.d.-a). *Shared responsibility model*. AWS. <https://aws.amazon.com/compliance/shared-responsibility-model/>
- Amazon Web Services. (n.d.-b). *What is cloud computing?* AWS. <https://aws.amazon.com/what-is-cloud-computing/>.
- Bộ Công an (2025). *Hướng dẫn số 12/HD-BCA về việc áp dụng các tiêu chuẩn an ninh mạng đối với hạ tầng điện toán đám mây phân tán*.
- Bộ Công an (2025). *Quyết định số 8297/QĐ-BCA-A05 ngày 09/10/2025 ban hành bộ tiêu chí đảm bảo an ninh mạng đối với nền tảng điện toán đám mây phục vụ Chính phủ điện tử, Chính quyền điện tử*.
- California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq. (2020/2023).
- Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025). *Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân*.
- Cloud Security Alliance. (n.d.). *STAR registry*. <https://cloudsecurityalliance.org/star>.
- European Data Protection Supervisor. (2018). *Guidelines on the use of cloud computing services by the European institutions and bodies*.
- General Services Administration. (n.d.). *Federal Risk and Authorization Management Program (FedRAMP)*. <https://www.fedramp.gov>.
- Hon, W. K., Millard, C., & Walden, I. (2012). Who is responsible for 'personal data' in cloud computing? The cloud of unknowing, Part 2. *International Data Privacy Law*, 2(1), 3–18. <https://doi.org/10.1093/idpl/ipr027>.
- IEEE Cloud Computing Initiative. (2014). *Understanding cloud computing standards and architecture*. IEEE Computer Society.
- National Institute of Standards and Technology. (2011). *Guidelines on security and privacy in public cloud computing* (NIST Special Publication 800-144).
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).
- Personal Data Protection Act 2012 (Singapore).
- Personal Data Protection Commission Singapore. (2021). *Advisory guidelines on key concepts in the PDPA*.
- Quốc hội (2025). *Luật Bảo vệ dữ liệu cá nhân*. Luật số: 91/2025/QH15, ngày 26/6/2025.
- Quốc hội (2025). *Luật An ninh mạng*. Số: 116/2025/QH15, ngày 10/12/2025.
- Quy định (EU) 2016/679 của Nghị viện châu Âu và Hội đồng ngày 27/4/2016 về bảo vệ thể nhân liên quan đến việc xử lý dữ liệu cá nhân và về việc tự do di chuyển dữ liệu đó (Quy định bảo vệ dữ liệu chung).
- Quy định (EU) 2023/2854 của Nghị viện châu Âu và Hội đồng về các quy tắc hài hòa đối với việc tiếp cận và sử dụng dữ liệu công bằng (Đạo luật Dữ liệu).
- Trần Minh Hải (2026). Chủ quyền số và quyền tài sản quốc gia đối với dòng dữ liệu xuyên biên giới dưới góc độ Luật An ninh mạng 2025. *Tạp chí Luật học*, (2), 34–42.
- Trần Quỳnh Anh, Chu Thị Thu Hà (2026). Pháp luật về bảo vệ dữ liệu cá nhân của khách hàng trong hợp đồng dịch vụ điện toán đám mây: Vương mắc và định hướng hoàn thiện. *Tạp chí pháp luật và phát triển* <https://phapluatphattrien.vn/phap-luat-viet-nam-ve-bao-ve-du-lieu-ca-nhan-cua-khach-hang-trong-hop-dong-dich-vu-dien-toan-dam-may-vuong-mac-va-dinh-huong-hoan-thien-d5406.html>.