

KINH NGHIỆM QUỐC TẾ VỀ TRÁCH NHIỆM PHÁP LÝ CỦA DOANH NGHIỆP CUNG CẤP DỊCH VỤ ĐIỆN TOÁN Đám Mây

HOÀNG MAI ANH*

Điện toán đám mây đang trở thành một cấu phần quan trọng của hạ tầng số, đặt ra yêu cầu hoàn thiện cơ chế xác định trách nhiệm pháp lý của doanh nghiệp cung cấp dịch vụ. Bài viết phân tích và so sánh kinh nghiệm của Liên minh châu Âu (EU), Hoa Kỳ, Trung Quốc và Singapore về trách nhiệm của doanh nghiệp cung cấp dịch vụ điện toán đám mây, tập trung vào các vấn đề bảo vệ dữ liệu và bảo đảm an ninh mạng. Bài viết chỉ ra khoảng trống trong các quy định hiện hành của Việt Nam và đề xuất các giải pháp hoàn thiện khung pháp lý theo hướng tiếp thu có chọn lọc kinh nghiệm quốc tế phù hợp với điều kiện Việt Nam.

Từ khóa: Trách nhiệm pháp lý; doanh nghiệp cung cấp dịch vụ; điện toán đám mây; bảo vệ dữ liệu; quản lý nhà nước.

Cloud computing is becoming a key component of digital infrastructure, creating a need to improve mechanisms for determining service providers' legal liability. This article analyzes and compares the experience of the European Union (EU), the United States, China, and Singapore regarding cloud service provider liability, focusing on data protection and ensuring cybersecurity. The article identifies gaps in Viet Nam's current regulations and proposes solutions to improve the legal framework by selectively drawing on international experience appropriate to Viet Nam's conditions.

Keywords: Legal liability; service providers; cloud computing; data protection; state management.

NGÀY NHẬN: 20/6/2026 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 20/9/2026 NGÀY DUYỆT ĐĂNG: 06/10/2026
Email: anhhm@hvpnv.edu.vn
DOI: <https://doi.org/10.59394/qlnn.370.2026.1669>

1. Đặt vấn đề

Cuộc cách mạng công nghiệp 4.0 thúc đẩy chuyển đổi số trên phạm vi toàn cầu, trong đó điện toán đám mây (Cloud Computing) ngày càng trở thành hạ tầng quan trọng của nền kinh tế số, phục vụ lưu trữ, xử lý dữ liệu và vận hành các nền tảng số. Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị xác định phát triển hạ tầng số hiện đại và hoàn thiện thể chế là những nhiệm vụ trọng tâm

của quá trình phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia (Bộ Chính trị, 2024).

Đặc thù kỹ thuật và cấu trúc cung cấp dịch vụ Cloud Computing với sự tham gia của nhiều chủ thể làm phát sinh những vấn đề phức tạp trong xác định trách nhiệm pháp lý

* ThS, Học viện Phụ nữ Việt Nam

khi xảy ra tranh chấp, sự cố an ninh mạng hoặc vi phạm liên quan đến thông tin, dữ liệu cá nhân. Việt Nam đã từng bước hình thành khung pháp lý về Cloud Computing thông qua *Luật Viễn thông* năm 2023 (Quốc hội, 2023) và các quy định về dữ liệu, bảo vệ dữ liệu cá nhân,

Trên cơ sở phân tích kinh nghiệm của EU, Hoa Kỳ, Trung Quốc và Singapore về trách nhiệm pháp lý của doanh nghiệp cung cấp dịch vụ Cloud Computing, bài viết tập trung làm rõ cách tiếp cận trong phân định trách nhiệm, bảo vệ dữ liệu và bảo đảm an ninh mạng; từ đó, rút ra một số bài học và đề xuất định hướng hoàn thiện pháp luật Việt Nam.

2. Khung trách nhiệm pháp lý

Khung trách nhiệm pháp lý phân tầng dựa trên mô hình dịch vụ Cloud Computing.

Dịch vụ Cloud Computing là loại hình dịch vụ công nghệ số, cung cấp các tài nguyên điện toán dùng chung thông qua Internet, chủ yếu theo ba mô hình: dịch vụ cơ sở hạ tầng (IaaS), dịch vụ nền tảng (PaaS) và dịch vụ phần mềm (SaaS). Theo nguyên tắc trách nhiệm chia sẻ, phạm vi trách nhiệm pháp lý của doanh nghiệp cung cấp dịch vụ tương ứng với mức độ kiểm soát kỹ thuật đối với hệ thống: từ hạ tầng ở IaaS, đến nền tảng ở PaaS và ứng dụng ở SaaS.

Đối với mô hình IaaS, doanh nghiệp cung cấp các tài nguyên điện toán được ảo hóa, như: máy chủ, bộ nhớ lưu trữ và hạ tầng mạng, còn khách hàng có mức độ kiểm soát cao nhất đối với hệ điều hành, ứng dụng và dữ liệu của mình (Khraisha, 2026; Umair, 2024). Doanh nghiệp phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ dữ liệu, chịu trách nhiệm nếu không chứng minh được đã thực hiện đầy đủ nghĩa vụ bảo mật theo tiêu chuẩn kỹ thuật (Ni Ketut Supasti Dharmawan & cộng sự, 2019); đồng thời, không được miễn trừ trách nhiệm nếu lỗi hỏng bảo mật hệ thống dẫn đến truy cập trái phép dữ liệu giữa các khách hàng do cùng sử

dụng chung hạ tầng (Tushar & cộng sự, 2026).

Đối với mô hình PaaS, doanh nghiệp kiểm soát nền tảng, hệ điều hành, phần mềm trung gian và môi trường thực thi; khách hàng chủ yếu chịu trách nhiệm đối với ứng dụng và dữ liệu (Umair, 2024). Vì vậy, doanh nghiệp phải bảo đảm tính ổn định, sẵn sàng và an toàn của nền tảng theo thỏa thuận cấp độ dịch vụ; đồng thời, bảo đảm phân tách giữa các không gian làm việc (Ni Ketut Supasti Dharmawan & cộng sự, 2019). Mô hình này cũng đòi hỏi hợp đồng xác định rõ quyền sở hữu đối với nền tảng, ứng dụng và dữ liệu nhằm hạn chế tranh chấp về quyền sở hữu trí tuệ (Nguyễn Như Hà, 2018).

Đối với mô hình SaaS, doanh nghiệp kiểm soát gần như toàn bộ hệ thống và tầng ứng dụng, còn khách hàng chủ yếu quản lý dữ liệu và quyền truy cập của người sử dụng (Umair, 2024). Do mức độ kiểm soát cao, trách nhiệm của doanh nghiệp về an toàn thông tin, bảo vệ dữ liệu cá nhân và quyền riêng tư cũng rộng hơn (Tushar & cộng sự, 2026). Tuy nhiên, các điều khoản giới hạn hoặc miễn trừ trách nhiệm trong hợp đồng theo mẫu có thể làm thu hẹp trách nhiệm thực tế của doanh nghiệp, nhất là đối với thiệt hại do mất dữ liệu hoặc sự cố an ninh mạng (Ni Ketut Supasti Dharmawan & cộng sự, 2019).

Như vậy, trách nhiệm pháp lý của doanh nghiệp cung cấp dịch vụ Cloud Computing thay đổi tương ứng với mức độ kiểm soát kỹ thuật, được mở rộng từ tầng hạ tầng trong IaaS, đến tầng nền tảng trong PaaS và đạt phạm vi rộng nhất trong SaaS. Việc xây dựng khung trách nhiệm pháp lý phân tầng là yêu cầu cần thiết nhằm bảo đảm phân định rõ ràng quyền và nghĩa vụ giữa các bên, qua đó nâng cao hiệu quả bảo vệ dữ liệu và thực thi pháp luật trong môi trường số.

3. Một số kinh nghiệm quốc tế

EU, Hoa Kỳ, Trung Quốc và Singapore đã hình thành các cơ chế pháp lý điều chỉnh trách nhiệm của doanh nghiệp cung cấp dịch vụ Cloud Computing, tập trung vào bảo vệ dữ

liệu, an ninh mạng và trách nhiệm hợp đồng nhưng có sự khác biệt về cách tiếp cận.

Tại EU là khu vực tiên phong xây dựng khung pháp lý toàn diện dựa trên bảo vệ các quyền cơ bản, trong đó quyền bảo vệ dữ liệu cá nhân được ghi nhận tại Điều 8 Hiến chương Quyền cơ bản của EU. Trọng tâm của khung pháp lý này là Quy định bảo vệ dữ liệu chung (GDPR) năm 2016. Theo GDPR, khách hàng sử dụng dịch vụ Cloud Computing được xác định là bên kiểm soát dữ liệu, còn doanh nghiệp cung cấp dịch vụ là bên xử lý dữ liệu; các bên ký kết Thỏa thuận xử lý dữ liệu, doanh nghiệp phải áp dụng các biện pháp kỹ thuật, tổ chức phù hợp để bảo vệ dữ liệu và thực hiện nghĩa vụ thông báo vi phạm dữ liệu trong thời hạn 72 giờ. Trường hợp vi phạm, doanh nghiệp có thể bị xử phạt đến 20 triệu euro hoặc 4% tổng doanh thu toàn cầu hàng năm theo Điều 83 GDPR (European Parliament & Council of the European Union, 2016). Bên cạnh GDPR, EU tăng cường trách nhiệm của doanh nghiệp thông qua Chỉ thị NIS2, *Đạo luật An ninh mạng* năm 2019, *Đạo luật Dữ liệu* năm 2023 và *Đạo luật Thị trường kỹ thuật số* (DMA) năm 2022. Cách tiếp cận của EU phù hợp với mô hình phân tầng trách nhiệm và cơ chế xử phạt gắn với doanh thu toàn cầu nâng cao hiệu quả răn đe, nhưng làm gia tăng chi phí tuân thủ, đặc biệt đối với doanh nghiệp nhỏ và vừa.

Tại Hoa Kỳ, pháp luật về bảo vệ dữ liệu được xây dựng theo hướng phân ngành và dựa nhiều vào cơ chế thị trường, thay vì một đạo luật liên bang có phạm vi điều chỉnh toàn diện. Ở cấp bang, CCPA và CPRA của California mở rộng quyền của người tiêu dùng đối với dữ liệu cá nhân, bao gồm: quyền tiếp cận, yêu cầu xóa và từ chối bán dữ liệu. Đáng chú ý, *Đạo luật Cloud* năm 2018 cho phép cơ quan thực thi pháp luật Hoa Kỳ yêu cầu doanh nghiệp cung cấp dữ liệu điện tử được lưu trữ ở nước ngoài, qua đó, có thể phát sinh xung đột với pháp luật về bảo vệ dữ liệu của các quốc gia khác, trong đó có GDPR

(California State Legislature, 2018; United States Congress, 2018). Mô hình này tạo không gian cho đổi mới và giảm gánh nặng tuân thủ, nhưng làm gia tăng sự phân mảnh pháp lý và nguy cơ xung đột thẩm quyền trong quản trị dữ liệu xuyên biên giới.

Tại Trung Quốc, pháp luật về dịch vụ Cloud Computing được xây dựng theo hướng đề cao chủ quyền mạng và an ninh *quốc gia, từng bước hoàn thiện với Luật An ninh mạng* năm 2017, *Luật An ninh dữ liệu* và *Luật Bảo vệ thông tin cá nhân* (PIPL) năm 2021. Các quy định này đặt ra yêu cầu chặt chẽ đối với doanh nghiệp cung cấp dịch vụ, bao gồm: bảo đảm an ninh hệ thống, mã hóa, sao lưu, lưu trữ nhật ký và hỗ trợ cơ quan nhà nước khi có yêu cầu. PIPL yêu cầu doanh nghiệp triển khai các biện pháp bảo vệ thông tin cá nhân và quy định mức xử phạt nghiêm khắc đối với hành vi vi phạm, có thể lên tới 50 triệu nhân dân tệ hoặc 5% doanh thu của năm trước (Ủy ban Thường vụ Đại hội đại biểu nhân dân toàn quốc, 2017, 2021a, 2021b). Cách tiếp cận này tăng cường khả năng kiểm soát dữ liệu và bảo đảm an ninh quốc gia, nhưng đồng thời có thể làm gia tăng chi phí tuân thủ và tạo thêm rào cản đối với hoạt động lưu chuyển dữ liệu xuyên biên giới.

Tại Singapore, pháp luật về dịch vụ Cloud Computing được xây dựng theo hướng thực dụng, dựa trên quản trị rủi ro nhằm cân bằng giữa bảo vệ dữ liệu, an ninh mạng và phát triển kinh tế số. Khung pháp lý, gồm: *Đạo luật Bảo vệ dữ liệu cá nhân* năm 2012 (PDPA), *Đạo luật An ninh mạng* năm 2018, *Đạo luật Lạm dụng máy tính* năm 1993 (CMA) và Tiêu chuẩn Singapore SS 584:2020 về an ninh Cloud Computing đa tầng; đồng thời, bổ sung các yêu cầu kỹ thuật về an ninh và phân định trách nhiệm trong các mô hình IaaS, PaaS và SaaS (Parliament of Singapore, 2012). Sự kết hợp giữa quy định pháp luật và tiêu chuẩn kỹ thuật tạo tính linh hoạt cho quản trị dịch vụ đám mây, nhưng cơ chế bảo vệ và chế tài vẫn

có những khác biệt đáng kể so với các chuẩn mực nghiêm ngặt như GDPR.

Nhìn tổng thể, bốn mô hình thể hiện những định hướng pháp lý khác nhau: EU nhấn mạnh bảo vệ quyền cơ bản và trách nhiệm giải trình; Hoa Kỳ thiên về điều chỉnh phân ngành và cơ chế thị trường; Trung Quốc đề cao chủ quyền dữ liệu và an ninh quốc gia; Singapore chú trọng quản trị rủi ro và cân bằng giữa bảo vệ dữ liệu với phát triển kinh tế số. Xét theo mức độ kiểm soát kỹ thuật trong các mô hình IaaS, PaaS và SaaS, EU và Singapore thể hiện rõ hơn sự gắn kết giữa trách nhiệm pháp lý với vai trò của chủ thể trong chuỗi cung ứng dịch vụ, trong khi Hoa Kỳ và Trung Quốc chủ yếu tiếp cận theo lĩnh vực và mức độ nhạy cảm của dữ liệu.

4. Những hạn chế, bất cập

Thứ nhất, pháp luật chưa phân định rõ trách nhiệm theo từng mô hình IaaS, PaaS và SaaS. Các quy định hiện hành chưa phản ánh đầy đủ sự khác biệt về mức độ kiểm soát kỹ thuật và dữ liệu của từng mô hình, gây khó khăn trong xác định trách nhiệm khi xảy ra sự cố. Đây là khoảng trống cần được khắc phục thông qua cơ chế phân tầng trách nhiệm, gắn nghĩa vụ của doanh nghiệp với mức độ kiểm soát thực tế đối với dữ liệu và hệ thống.

Thứ hai, cơ chế thỏa thuận xử lý và thông báo vi phạm dữ liệu chưa được cụ thể hóa đầy đủ. Pháp luật chưa quy định rõ DPA như một công cụ pháp lý chuyên biệt, trong khi các nội dung về xử lý dữ liệu chủ yếu được thỏa thuận trong hợp đồng; thời hạn và cơ chế thông báo khi xảy ra vi phạm cũng chưa được quy định thống nhất. Điều này có thể dẫn đến bất cân xứng về trách nhiệm giữa nhà cung cấp và khách hàng.

Thứ ba, khung pháp lý và tiêu chuẩn kỹ thuật còn phân tán. Trách nhiệm của doanh nghiệp cung cấp dịch vụ Cloud Computing hiện được quy định trong nhiều văn bản chuyên ngành, trong khi chưa có tiêu chuẩn kỹ thuật quốc gia chuyên biệt về an ninh Cloud Computing đa tầng. Sự phân tán này

làm giảm tính thống nhất và gây khó khăn cho kiểm tra, đánh giá tuân thủ.

Thứ tư, các chế tài chưa bảo đảm đầy đủ tính tương xứng với quy mô và mức độ tác động của vi phạm. Việc chủ yếu áp dụng mức phạt cố định có thể hạn chế hiệu quả răn đe đối với doanh nghiệp có quy mô hoạt động lớn. Việt Nam cần nghiên cứu cơ chế chế tài linh hoạt hơn, bảo đảm tương xứng với tính chất, mức độ vi phạm và quy mô hoạt động của doanh nghiệp, đồng thời phù hợp với điều kiện thị trường và năng lực thực thi pháp luật.

5. Một số kinh nghiệm cho Việt Nam

Một là, xây dựng cơ chế phân tầng trách nhiệm pháp lý theo từng mô hình dịch vụ. Cần hoàn thiện pháp luật theo hướng phân định rõ trách nhiệm của doanh nghiệp cung cấp IaaS, PaaS và SaaS trên cơ sở mức độ kiểm soát đối với hạ tầng, nền tảng, ứng dụng và dữ liệu. Nhà cung cấp có mức độ kiểm soát kỹ thuật càng cao cần chịu trách nhiệm tương ứng về bảo mật, quản lý dữ liệu, phòng ngừa và xử lý sự cố. Cách tiếp cận này giúp xác định rõ trách nhiệm giữa doanh nghiệp và khách hàng, hạn chế khoảng trống hoặc chồng lấn trách nhiệm khi xảy ra vi phạm.

Hai là, hoàn thiện cơ chế thỏa thuận xử lý và thông báo vi phạm dữ liệu. Cần quy định rõ trách nhiệm của các bên trong DPA tối thiểu, gồm: phạm vi và mục đích xử lý dữ liệu; quyền, nghĩa vụ của các bên; biện pháp bảo đảm an toàn; quản lý bên thứ ba; xử lý dữ liệu khi chấm dứt hợp đồng; cơ chế phối hợp và trách nhiệm bồi thường khi xảy ra vi phạm. Đồng thời, cần xác định cụ thể thời hạn, phương thức và nội dung thông báo vi phạm, bảo đảm khách hàng và cơ quan có thẩm quyền có đủ thông tin để kịp thời ứng phó, hạn chế thiệt hại.

Ba là, hoàn thiện khung pháp lý và tiêu chuẩn kỹ thuật về an ninh Cloud Computing. Cần nghiên cứu xây dựng văn bản quy phạm pháp luật chuyên biệt về dịch vụ điện toán đám mây hoặc hoàn thiện các quy định hiện hành theo hướng thống nhất trách nhiệm của

doanh nghiệp cung cấp dịch vụ. Xây dựng và hoàn thiện tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh Cloud Computing theo các mô hình IaaS, PaaS và SaaS, làm cơ sở cho doanh nghiệp triển khai biện pháp bảo mật và cho cơ quan quản lý kiểm tra, đánh giá mức độ tuân thủ.

Bốn là, hoàn thiện cơ chế thanh tra, kiểm tra, giám sát và xử lý vi phạm. Quản lý nhà nước đối với dịch vụ Cloud Computing cần chuyển mạnh sang phương thức quản trị dựa trên rủi ro, tập trung vào các dịch vụ, hệ thống và loại dữ liệu có mức độ rủi ro cao. Cơ quan quản lý cần tăng cường phối hợp trong thanh tra, kiểm tra, giám sát việc tuân thủ; đồng thời, hoàn thiện chế tài theo hướng bảo đảm tính tương xứng với tính chất, mức độ vi phạm, quy mô hoạt động và khả năng gây thiệt hại của doanh nghiệp.

Năm là, nâng cao năng lực bảo đảm an toàn dữ liệu của doanh nghiệp và nhận thức của khách hàng. Bên cạnh hoàn thiện pháp luật, cần khuyến khích doanh nghiệp đầu tư cho nhân lực, công nghệ, quy trình quản trị rủi ro và khả năng ứng phó sự cố; đồng thời, tăng cường hướng dẫn khách hàng nhận diện rủi ro, lựa chọn nhà cung cấp và kiểm soát việc xử lý dữ liệu. Việc nâng cao năng lực của cả bên cung cấp và bên sử dụng sẽ góp phần chuyển các yêu cầu pháp lý thành năng lực bảo vệ dữ liệu trên thực tế.

Sáu là, tăng cường hợp tác và hài hòa pháp luật về dữ liệu xuyên biên giới. Trong bối cảnh dịch vụ Cloud Computing có tính xuyên biên giới cao, Việt Nam cần tiếp tục nghiên cứu kinh nghiệm quốc tế, nhất là các cơ chế về chuyển dữ liệu, trách nhiệm của nhà cung cấp và xử lý sự cố. Đồng thời, thúc đẩy hợp tác với các quốc gia và tổ chức quốc tế nhằm nâng cao khả năng phối hợp, chia sẻ thông tin và xử lý các vi phạm liên quan đến dữ liệu xuyên biên giới□

Tài liệu tham khảo:

Bộ Chính trị (2024). *Nghị quyết số 57 - NQ/TW*

ngày 22/12/2024 về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

California State Legislature (2018). *California Consumer Privacy Act (CCPA)*. California.

European Parliament & Council of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)*. Official Journal of the European Union.

Khraisha, W (2026). Cybersecurity in cloud industry: Legal obligations and liabilities under European regulations and technological advancements. *Belügyi Szemle*, 74(1).

Nguyễn Như Hà (2018). Các vấn đề pháp lý chính phát sinh từ điện toán đám mây. *Tạp chí Phát triển Khoa học và Công nghệ: Kinh tế - Luật và Quản lý*, 2(3).

Ni Ketut Supasti Dharmawan, Kasih, D. P. D., & Stiawan, D. (2019). Personal data protection and liability of internet service provider: A comparative approach. *International Journal of Electrical and Computer Engineering (IJECE)*, 9(4).

Parliament of Singapore (2012). *Personal Data Protection Act 2012 (PDPA)*. Singapore.

Tushar, Pradhan, N., Shrivastava, P. C., Jaiswal, P., Singh, S., & Mishra, V (2026). Legal challenges in cloud computing. Trong *A research agenda for cybersecurity law and policy*. IGI Global Scientific Publishing.

Umair, M (2024). Protecting data access liabilities in cloud computing. *Journal of Artificial Intelligence General Science (JAIGS)*, 3(1).

United States Congress (2018). *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*. Washington, D.C.

Ủy ban Thường vụ Đại hội đại biểu nhân dân toàn quốc (2017). *Luật An ninh mạng của nước Cộng hòa Nhân dân Trung Hoa*. Bắc Kinh.

Ủy ban Thường vụ Đại hội đại biểu nhân dân toàn quốc (2021a). *Luật An ninh dữ liệu của nước Cộng hòa Nhân dân Trung Hoa*. Bắc Kinh.

Ủy ban Thường vụ Đại hội đại biểu nhân dân toàn quốc (2021b). *Luật Bảo vệ thông tin cá nhân của nước Cộng hòa Nhân dân Trung Hoa*. Bắc Kinh.