Ngày 09 tháng 7 năm 2026

Ý KIẾN ĐÓNG GÓP CỦA BSA ĐỐI VỚI DỰ THẢO LUẬT AN NINH DỮ LIỆU

Kính gửi: Bộ Công an

Liên minh Phần mềm (**BSA**)[1] trân trọng cảm ơn Bộ Công an đã tạo cơ hội để chúng tôi tham gia đóng góp ý kiến về việc xây dựng Luật An ninh dữ liệu. BSA là hiệp hội thương mại toàn cầu của ngành công nghiệp phần mềm. Các thành viên của chúng tôi là những công ty dẫn đầu trong lĩnh vực trí tuệ nhân tạo (**AI**), an ninh mạng, điện toán đám mây, và các công nghệ tiên tiến khác. Trong những năm qua, chúng tôi đã tích cực tham gia cùng Bộ Công an trong lĩnh vực an ninh mạng,[2] bảo vệ dữ liệu cá nhân,[3] và các văn bản pháp luật khác liên quan đến việc quản trị dữ liệu.[4]

Chủ Quyền Dữ Liệu Quốc Gia

Hồ Sơ Chính Sách của dự án Luật An ninh dữ liệu định hướng áp dụng mô hình quản trị dựa trên rủi ro và phân lớp bảo vệ nhằm xây dựng một "hệ sinh thái tự chủ, tự cường" theo đó: (1) đối với nhóm Dữ Liệu Cốt Lõi thì yêu cầu phải sử dụng mật mã nội địa và hạ tầng dùng riêng (air-gapped); (2) đối với nhóm Dữ Liệu Quan Trọng thì yêu cầu phải lưu trữ dữ liệu "gốc" tại Việt Nam; và (3) đối với nhóm dữ liệu còn lại được phép "lưu thông linh hoạt" sử dụng cơ chế quản lý bằng "hậu kiểm" và tuân theo tiêu chuẩn an toàn thông lệ quốc tế. Theo Hồ Sơ Chính Sách, điều này cho phép Việt Nam giữ vững được độc lập tự chủ trên không gian mạng, giữ vững được chủ quyền số song không bị tụt hậu trong cuộc đua kinh tế toàn cầu.

Hồ Sơ Chính Sách đồng thời đề ra các bước thực thi dưới đây để đảm bảo chủ quyền số:

- Xây dựng danh mục dữ liệu quốc gia, phân loại rõ ràng các nhóm dữ liệu để áp dụng cấp độ bảo vệ tương ứng, tránh đánh đồng dữ liệu kinh doanh với dữ liệu an ninh.

[1] Các thành viên của BSA bao gồm: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] Ví dụ, BSA đã tham dự Hội thảo về Dự thảo Nghị định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng do Bộ Công an tổ chức vào tháng 11 năm 2022. Gần đây nhất, BSA đã gửi ý kiến góp ý về lĩnh vực an ninh mạng vào ngày 6 tháng 3 năm 2026 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-draft-decree-detailing-articles-cybersecurity-law.

[3] Ví dụ, BSA đã trình bày quan điểm tại Hội thảo về Bảo vệ dữ liệu cá nhân do Bộ Công an tổ chức vào tháng 6 năm 2024. Gần đây nhất, BSA đã gửi ý kiến góp ý về bảo vệ dữ liệu cá nhân vào ngày 3 tháng 10 năm 2025 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-decree-on-the-law-on-personal-data-protection.

[4] Xem Ý kiến góp ý của BSA đối với Dự thảo Nghị định và Dự thảo Quyết định hướng dẫn thi hành Luật Dữ liệu ngày 17 tháng 3 năm 2025 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-decree-and-draft-decision-to-implement-the-data-law, và Ý kiến góp ý của BSA đối với Dự thảo Luật Dữ liệu ngày 4 tháng 9 năm 2024 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-data-law.

- Thiết lập "biên giới số" thông minh: vận hành đơn vị quản trị an ninh dữ liệu quốc gia để theo dõi dòng chảy dữ liệu tự động 24/7, phát hiện bất thường và không cần đọc nội dung dữ liệu của doanh nghiệp.
- Làm chủ hạ tầng lưu trữ: ban hành các quy chuẩn kỹ thuật bắt buộc để các nhà cung cấp dịch vụ hạ tầng trong nước đạt tiêu chuẩn bảo vệ dữ liệu.
- Có thể nghiên cứu cơ chế "hậu kiểm kỹ thuật số", thay thế giấy phép bằng việc giám sát trực tuyến và thanh tra dựa trên dấu hiệu vi phạm.

BSA ủng hộ mục tiêu của Việt Nam trong việc nâng cao năng lực tự cường, tạo lập niềm tin và thúc đẩy đổi mới, sáng tạo. Tuy nhiên, không thể đạt được chủ quyền số thiết thực thông qua việc hạn chế hợp tác toàn cầu hay giới hạn các lựa chọn về công nghệ. Chủ quyền số cần được xây dựng dựa trên các tiêu chuẩn được quốc tế công nhận, quản trị minh bạch và khả năng vận hành một cách vững chắc trong một hệ sinh thái số mở và có tính kết nối. Thách thức đối với các nhà lập pháp là phải dung hoà được mong muốn kiểm soát chính đáng của Việt Nam với thực tiễn của một nền kinh tế số toàn cầu vốn phụ thuộc lẫn nhau.

Khuyến nghị: Các cơ chế kiểm soát liên quan đến chủ quyền chỉ nên được áp dụng theo mức độ rủi ro, trên cơ sở cân nhắc toàn diện các hệ quả đi kèm, ví dụ như khả năng đổi mới, sáng tạo, an ninh mạng và mức độ khả dụng của các tính năng dịch vụ. Suy cho cùng, từng tổ chức riêng biệt – tùy thuộc vào mức độ rủi ro và tác động tiềm tàng, và dù là cơ quan nhà nước hay đơn vị vận hành hạ tầng trọng yếu – phải là chủ thể tự quyết định phạm vi áp dụng biện pháp quản lý và phương án cân đối các rủi ro và hệ quả ảnh hưởng này.

Bảo Đảm An Ninh Dữ Liệu

Luật An ninh dữ liệu đề xuất bảo đảm an ninh dữ liệu dựa trên cơ chế phân loại 04 cấp độ rủi ro, cụ thể:

- Cấp độ 1: Dữ liệu tác động trực tiếp đến độc lập, chủ quyền, quốc phòng, an ninh và sự ổn định của chế độ. Dữ liệu Cấp độ 1 đồng thời được xem là Dữ Liệu Cốt Lõi.
- Cấp độ 2: Dữ liệu tác động trực tiếp đến sự vận hành của hạ tầng thông tin quốc gia, trật tự an toàn xã hội và nền kinh tế vĩ mô.
- Cấp độ 3: Dữ liệu tác động đến quyền riêng tư, danh dự của công dân và lợi ích hợp pháp của tổ chức trên quy mô lớn.
- Cấp độ 4: Các loại dữ liệu công khai, thương mại có mức độ ảnh hưởng thấp nhưng vẫn phải được quản lý, bảo vệ theo quy định của pháp luật.

Cấp độ 1 và 2 yêu cầu áp dụng biện pháp kỹ thuật đặc biệt, bao gồm bắt buộc áp dụng công nghệ "lá chắn dữ liệu", cô lập vật lý đối với dữ liệu tuyệt mật và kiểm soát quyền truy cập dựa trên định danh sinh trắc học quốc gia. Đối với cấp độ 1 và 2 thì phải sử dụng hạ tầng dùng riêng, mật mã nội địa và kiểm soát truy cập đa nhân tố đặc biệt. Cấp độ 3 và 4 sẽ sử dụng hạ tầng dùng chung có tính linh hoạt cao, ưu tiên tốc độ kết nối và chia sẻ. Hồ Sơ Chính Sách đề cập rằng "[p]hân thành 4 cấp độ giúp dữ liệu cấp độ 3, 4 được lưu thông cực nhanh, thúc đẩy xã hội số, kinh tế số". Thêm

vào đó, Luật An ninh dữ liệu hướng tới việc ưu tiên sử dụng các giải pháp phần cứng, phần mềm và mật mã nội địa để loại bỏ nguy cơ "cửa sau" từ các nhà cung cấp nước ngoài.

Nếu một lượng lớn dữ liệu do các tổ chức thuộc khu vực tư nhân nắm giữ bị phân loại vào Cấp độ 1 hoặc Cấp độ 2, ví dụ như dữ liệu trong lĩnh vực tài chính hoặc y tế, việc chuyển và sử dụng dữ liệu này có thể gặp điểm nghẽn; làm chậm lại các hoạt động thương mại, giảm khả năng bảo mật và ảnh hưởng đến quá trình đổi mới sáng tạo.

Việt Nam đã ban hành Luật Dữ liệu theo đó phân loại dữ liệu thành ba nhóm: Dữ Liệu Cốt Lõi, Dữ Liệu Quan Trọng và Dữ liệu khác. Luật An ninh dữ liệu cần làm rõ mối tương quan giữa các nhóm dữ liệu theo Luật Dữ liệu và đề xuất phân loại theo hệ thống bốn cấp theo Luật An ninh dữ liệu. Để tránh nguy cơ chồng chéo pháp luật, Việt Nam nên xem xét sửa đổi, bổ sung các luật hiện hành thay vì ban hành một Luật An ninh dữ liệu riêng rẽ. Phương án này sẽ giúp hợp lý hóa các quy định quản trị dữ liệu hiện tại, loại bỏ các nghĩa vụ trùng lặp cho doanh nghiệp, đồng thời hình thành một hành lang pháp lý đồng bộ, nhất quán về phân loại, bảo vệ và chuyển dữ liệu xuyên biên giới.

Khuyến nghị: Để tránh tình trạng phân loại quá mức gây cản trở cho các hoạt động kinh tế, Luật An ninh dữ liệu cần thu hẹp phạm vi và áp dụng phương thức tiếp cận dựa trên mức độ rủi ro. Theo đó, dữ liệu Cấp độ 1 và Cấp độ 2 cần được định nghĩa rõ ràng và chủ yếu giới hạn đối với dữ liệu thuộc quyền sở hữu hoặc kiểm soát của Nhà nước mà có ảnh hưởng trực tiếp đến quốc phòng, an ninh quốc gia, an toàn công cộng, hoặc sự vận hành của các hạ tầng trọng yếu quốc gia. Các nhóm dữ liệu phổ biến ở khu vực tư nhân như dữ liệu tài chính hoặc dữ liệu y tế không đương nhiên bị phân loại là dữ liệu Cấp độ 1 hoặc Cấp độ 2. Dữ liệu cũng không nên bị phân loại là cốt lõi hay quan trọng chỉ dựa trên quy mô hoặc khối lượng dữ liệu. Việc phân loại một cách bao quát toàn bộ các ngành hoặc bao gồm cả các bộ dữ liệu thông thường thuộc nhóm thương mại, vận hành hay khách hàng là dữ liệu Cấp độ 1 và 2 sẽ tạo ra chính các điểm nghẽn dữ liệu mà Hồ Sơ Chính Sách muốn tránh. Thêm vào đó, chúng tôi kiến nghị thu hẹp phạm vi của dữ liệu Cấp độ 1 và 2, ví dụ như định nghĩa dữ liệu Cấp độ 1 là những dữ liệu có liên quan trực tiếp đến các vấn đề quân sự hoặc các vấn đề nhạy cảm về an ninh quốc gia, đồng thời loại bỏ các khái niệm mang nghĩa rộng như "độc lập" và "trật tự an toàn xã hội".

Khuyến nghị: Luật An ninh dữ liệu không nên quy định rõ việc ưu tiên sử dụng phần cứng và phần mềm nội địa vì điều này sẽ làm hạn chế khả năng tiếp cận của các tổ chức tại Việt Nam đối với các giải pháp công nghệ tiên tiến hàng đầu trên thế giới, bao gồm các công nghệ bảo mật hiện đại, đồng thời cản trở khả năng hội nhập liền mạch của các tổ chức Việt Nam vào nền kinh tế số toàn cầu. Thay vào đó, Luật An ninh dữ liệu nên ưu tiên áp dụng các tiêu chuẩn quốc tế được công nhận rộng rãi, bảo đảm mức độ cao về khả năng tương thích, liên thông giữa các hệ thống cũng như an toàn, an ninh dữ liệu.

Khuyến nghị: Luật An ninh dữ liệu nên ưu tiên thúc đẩy quá trình chuyển đổi sang các giải pháp mật mã hậu lượng tử (**Post-Quantum Cryptography - PQC**) thông qua việc tương thích với các tiêu chuẩn được quốc tế công nhận và các nỗ lực chuyển đổi đang được triển khai trên phạm vi toàn cầu. Việt Nam nên hỗ trợ phát triển các tiêu chuẩn toàn cầu cùng các chính sách, tiêu chuẩn kỹ thuật và lộ trình chuyển đổi theo hướng bảo đảm an toàn trước các rủi ro từ điện toán lượng tử, đồng thời duy trì khả năng tương thích và liên thông quốc tế; tránh áp dụng các cách tiếp cận

mang tính đặc thù quốc gia có thể làm suy giảm khả năng tương tác, cản trở đổi mới sáng tạo và ảnh hưởng đến an ninh.

Đảm Bảo An Ninh trong Chuyển Dữ Liệu Xuyên Biên Giới

Hồ Sơ Chính Sách nhấn mạnh mục tiêu chính sách bao gồm việc thực thi chủ quyền số và bảo đảm an ninh quốc gia, đồng thời làm rõ yêu cầu lưu trữ dữ liệu nhạy cảm tại Việt Nam "đảm bảo rằng cơ quan quản lý luôn có khả năng tiếp cận, kiểm soát và bảo vệ tài nguyên này trước các nguy cơ can thiệp hoặc cấm vận từ bên ngoài". Hồ Sơ Chính Sách cũng nêu mục tiêu thiết lập cơ chế quản trị dòng chảy dữ liệu "mở có kiểm soát" và chuyển đổi từ tư duy "cấm đoán" sang "điều phối dựa trên rủi ro". Hồ Sơ Chính Sách hướng tới việc tạo ra các "luồng xanh" cho dữ liệu thông thường để phát triển kinh tế, đồng thời thiết lập các "luồng đỏ" kiểm soát chặt chẽ dữ liệu cốt lõi và quan trọng, điều này sẽ tạo sự linh hoạt cho nền kinh tế dữ liệu nhưng không đánh đổi an ninh quốc gia. Tuy nhiên, các hạn chế đối với dòng chảy dữ liệu và chuyển dữ liệu có thể vô tình làm giảm hiệu quả của các cơ chế dự phòng hệ thống được tích hợp trong các dịch vụ điện toán đám mây tiên tiến, hệ quả là, dữ liệu quan trọng có thể đối mặt với rủi ro mất mát lớn hơn trong trường hợp xảy ra các sự cố hoặc tình huống ngoài dự kiến[5] ảnh hưởng đến các hệ thống lưu trữ dữ liệu được yêu cầu đặt tại địa phương.

Chúng tôi đánh giá cao việc Bộ Công an tập trung vào việc thúc đẩy hội nhập và tương thích quốc tế như nội luật hóa các cam kết quốc tế về Dòng Chảy Dữ Liệu Tự Do Có Tin Cậy (**Data Free Flow with Trust – DFFT**) và các hiệp định thương mại tự do thế hệ mới như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (**Comprehensive and Progressive Agreement for Trans-Pacific Partnership – CPTPP**), Hiệp định Thương mại Tự do Liên minh châu Âu – Việt Nam (**EU-Vietnam Free Trade Agreement – EVFTA**); và Hiệp định Khung về Kinh tế số ASEAN (**ASEAN Digital Economy Framework Agreement – DEFA**).

Mặc dù chúng tôi thừa nhận một số lợi ích của cơ chế "danh sách trắng" (danh sách các quốc gia/tổ chức có hệ thống pháp luật bảo vệ dữ liệu tương đương Việt Nam, doanh nghiệp chuyển dữ liệu sang các đối tượng này chỉ cần thông báo, không cần xin phép với cơ quan nhà nước), chúng tôi vẫn có những quan ngại liên quan đến nghĩa vụ thông báo cho cơ quan nhà nước, quy trình lập danh sách được chấp thuận cũng như cách thức quản lý đối với các chủ thể không nằm trong danh sách này. Chẳng hạn, nếu yêu cầu thông báo cho cơ quan nhà nước vẫn kéo theo nghĩa vụ nộp các bộ hồ sơ phức tạp như các yêu cầu hiện hành theo Luật Bảo vệ dữ liệu cá nhân và Luật Dữ liệu, thì cơ chế danh sách trắng sẽ khó đạt được mục tiêu mong muốn là giảm gánh nặng tuân thủ cho doanh nghiệp. Tương tự, nếu quy trình đưa các quốc gia hoặc tổ chức vào danh sách được chấp thuận mang tính hạn chế quá mức hoặc mất nhiều thời gian, thì cách tiếp cận này trên thực tế có thể tạo ra nhiều rào cản đối với hoạt động chuyển dữ liệu xuyên biên giới hơn mức cần thiết.

Việt Nam đồng thời chuyển đổi từ "tiền kiểm" sang "hậu kiểm" số bằng cách giới thiệu "Điều Khoản Mẫu" cho doanh nghiệp và cơ chế liên thông quốc tế như Hệ Thống Quy Tắc Bảo Mật Xuyên Biên Giới Toàn Cầu (**Global Cross-Border Privacy Rules System – Global CBPR**) mà theo đó dữ liệu Việt Nam có thể lưu chuyển trong các khối liên minh kinh tế mà không cần đàm phán lại từ

[5] Tham khảo thêm ví dụ tại: https://www.straitstimes.com/asia/east-asia/up-in-smoke-work-documents-of-191000-civil-servants-lost-in-data-centre-fire-in-south-korea

đầu. Tương tự, nếu doanh nghiệp vẫn bị yêu cầu lập và nộp các bộ hồ sơ chi tiết đối với từng lần chuyển dữ liệu, thì các mục tiêu đặt ra sẽ khó có thể đạt được.

BSA đặc biệt ủng hộ việc tạo điều kiện thuận lợi cho hoạt động chuyển dữ liệu xuyên biên giới, bao gồm cả dữ liệu cá nhân. Chúng tôi ghi nhận và đánh giá cao việc cả Hồ sơ Dự thảo Báo Cáo Đánh Giá Tác Động Chính Sách và Dự thảo Báo cáo thực trạng bảo vệ dữ liệu cá nhân đều thừa nhận tầm quan trọng của hoạt động chuyển dữ liệu quốc tế, bao gồm trong bối cảnh thực hiện các cam kết của Việt Nam theo CPTPP và EVFTA.

Khuyến nghị: Chúng tôi đặc biệt khuyến nghị Luật An ninh dữ liệu không nên đặt ra bất kỳ yêu cầu mới nào đối với hoạt động chuyển dữ liệu xuyên biên giới. Thay vào đó, Luật An ninh dữ liệu nên được xem là cơ hội để rà soát, hợp lý hóa và thống nhất các nghĩa vụ liên quan đến việc chuyển dữ liệu hiện đang tồn tại và có sự chồng chéo giữa Luật Bảo vệ dữ liệu cá nhân và Luật Dữ liệu. Luật An ninh dữ liệu theo đó cần thiết lập một khuôn khổ pháp lý thống nhất, đồng bộ thay vì bổ sung thêm một tầng nghĩa vụ tuân thủ mới. Hồ Sơ Chính Sách đã xác định tình trạng phân mảnh pháp lý và chồng chéo nghĩa vụ là "một trong những hạn chế lớn nhất" của khuôn khổ quản trị dữ liệu hiện nay. Việc đưa ra thêm những yêu cầu về chuyển giao – ngay cả khi chỉ là những điều chỉnh để hoàn thiện – cũng làm gia tăng rủi ro làm phân mảnh nghĩa vụ mà Luật An ninh dữ liệu đang muốn khắc phục. Doanh nghiệp đã đầu tư nguồn lực để xây dựng hệ thống tuân thủ đối với hoạt động chuyển dữ liệu theo Luật Bảo vệ dữ liệu cá nhân không nên phải đối mặt với một hệ thống nghĩa vụ thứ hai có khả năng chồng chéo hoặc mâu thuẫn đối với cùng một loại hoạt động là chuyển dữ liệu.

Luật An ninh dữ liệu cần làm rõ rằng việc dữ liệu chỉ được định tuyến về mặt kỹ thuật hoặc được xử lý tạm thời thông qua hạ tầng đặt ngoài lãnh thổ Việt Nam, tự thân nó không được xem là hoạt động chuyển dữ liệu xuyên biên giới thuộc phạm vi điều chỉnh của pháp luật. Luật An ninh dữ liệu cũng cần quy định rằng không bắt buộc phải thực hiện hoạt động xử lý dữ liệu gốc trên lãnh thổ Việt Nam nếu việc truy cập từ xa đối với dữ liệu nhạy cảm vẫn có thể đáp ứng các mục tiêu chính sách của Việt Nam về bảo đảm chủ quyền số và an ninh quốc gia. Ngoài ra, trong trường hợp việc đánh giá tác động đối với hoạt động xử lý và chuyển dữ liệu xuyên biên giới được yêu cầu áp dụng trong những hoàn cảnh cụ thể, các báo cáo đánh giá này chỉ nên phải nộp cho Bộ Công an khi có yêu cầu thay vì bắt buộc phải nộp trong mọi trường hợp. Cách tiếp cận này phù hợp với thông lệ quốc tế và sẽ giúp cả doanh nghiệp lẫn cơ quan quản lý tập trung nguồn lực hiệu quả hơn vào các trường hợp thực sự cần được xem xét và quản lý.

Đây là thời điểm vàng để Việt Nam công nhận và áp dụng các cơ chế chuyển dữ liệu cá nhân được quốc tế công nhận mà không áp đặt thêm các yêu cầu tuân thủ bổ sung, chẳng hạn như nghĩa vụ thực hiện Đánh Giá Tác Động Chuyển Dữ Liệu Cá Nhân theo Luật Bảo vệ dữ liệu cá nhân. Những cơ chế này bao gồm Điều Khoản Hợp Đồng Chuẩn của Liên minh Châu Âu (**EU Standard Contractual Clauses – EU SCCs**), Điều Khoản Hợp Đồng Mẫu của Hiệp hội các quốc gia Đông Nam Á (**ASEAN Model Contractual Clauses – ASEAN MCCs**), và Global CBPR. Việc công nhận các cơ chế này sẽ góp phần giảm gánh nặng quản lý và tuân thủ cho cả doanh nghiệp và cơ quan quản lý nhà nước, tạo thuận lợi cho dòng chảy dữ liệu xuyên biên giới đáng tin cậy, đồng thời thúc đẩy các mục tiêu của Việt Nam về hội nhập quốc tế và phát triển kinh tế số.

Trong trường hợp Việt Nam không lựa chọn cách tiếp cận này, thì cũng cần loại bỏ các yêu cầu báo cáo trùng lặp và tránh bổ sung thêm các nghĩa vụ báo cáo mới đối với hoạt động chuyển dữ

liệu xuyên biên giới. Điều này dẫn đến sự chồng chéo không cần thiết và làm gia tăng gánh nặng tuân thủ mà không mang lại lợi ích tương ứng về an ninh, an toàn dữ liệu. Luật An ninh dữ liệu cần bổ sung một quy định rõ ràng về nguyên tắc không trùng lặp, theo đó, trong trường hợp một hoạt động chuyển dữ liệu đã thuộc phạm vi điều chỉnh của các yêu cầu theo Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu hoặc bất kỳ văn bản pháp luật nào khác, thì chỉ cần thực hiện một lần báo cáo đối với hoạt động chuyển dữ liệu này.

Bảo Đảm An Ninh trong Trí Tuệ Nhân Tạo (AI) Và Ứng Dụng Công Nghệ Mới

Một trong những mục tiêu chính sách của Luật An ninh dữ liệu là việc ứng dụng và phát triển AI cùng các công nghệ mới, đặc biệt là khuyến khích phát triển các mô hình ngôn ngữ lớn và hệ thống AI "thuần Việt" và giảm thiểu sự lệ thuộc vào các thuật toán nước ngoài. Việc thiết lập các hệ thống AI nội địa – bao gồm tùy chỉnh các mô hình AI để hỗ trợ ngôn ngữ địa phương và cung cấp các dịch vụ phù hợp hơn với nhu cầu trong nước – là một mục tiêu đáng ghi nhận. Tuy nhiên, việc giới hạn quyền tiếp cận hoặc sử dụng các công nghệ này cho các doanh nghiệp trong nước hoặc doanh nghiệp phát triển công nghệ nội địa sẽ làm hạn chế những nỗ lực đổi mới sáng tạo và phát triển năng lực công nghệ tự chủ của Việt Nam.

Để lấy ví dụ, Luật An ninh dữ liệu nên cân nhắc về thực trạng hệ thống pháp luật Việt Nam có thể vô tình làm hạn chế sự đổi mới sáng tạo của AI trong nước, ví dụ trong các quy định về sở hữu trí tuệ (**SHTT**) và Nghị định hướng dẫn thi hành Luật SHTT. BSA gần đây đã gửi ý kiến góp ý[6] trong đó khuyến nghị: (1) đảm bảo không giới hạn ngoại lệ sử dụng văn bản và dữ liệu Việt Nam cho cả mục đích thương mại và mục đích phi thương mại; và (2) loại bỏ yêu cầu buộc nhà phát triển mô hình bảo đảm rằng đầu ra của hệ thống AI không cạnh tranh với nội dung của chủ thể quyền, cùng với một số khuyến nghị khác.

Khuyến nghị: Nếu mục tiêu của Luật An ninh dữ liệu là khuyến khích phát triển các mô hình ngôn ngữ quy mô lớn và các hệ thống AI trong nước, Việt Nam cần bảo đảm rằng khuôn khổ pháp luật nói chung tạo điều kiện thuận lợi cho hoạt động đổi mới sáng tạo trong lĩnh vực AI. Đặc biệt, Chính phủ Việt Nam nên xem xét các khuyến nghị của BSA liên quan đến Luật Sở hữu trí tuệ và Nghị định hướng dẫn thi hành, bao gồm việc cho phép hoạt động khai thác văn bản và dữ liệu (text-and-data mining) phục vụ mục đích thương mại và loại bỏ các hạn chế làm cản trở việc phát triển, triển khai AI trên thực tế. Các quy định mang tính hạn chế đối với hoạt động khai thác văn bản và dữ liệu có thể vô tình cản trở sự phát triển của chính các năng lực AI trong nước mà Luật An ninh dữ liệu đang hướng tới thúc đẩy.

Hồ Sơ Chính Sách đề cập rằng Luật An ninh dữ liệu sẽ xác lập trách nhiệm pháp lý rõ ràng của các chủ thể phát triển và vận hành AI đối với các hệ quả do thuật toán gây ra, bảo vệ nền tảng tư tưởng và an ninh xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Thêm vào đó, Hồ Sơ Chính Sách xác lập 04 cấp độ rủi ro của AI, quy định dán nhãn bắt buộc đối với nội dung do AI tạo ra, và các yêu cầu khác. Tuy nhiên, những nội dung này đã được đề cập tại Luật Trí tuệ nhân tạo.

[6] Ý kiến góp ý của BSA đối với Dự thảo Nghị định hướng dẫn Luật Sở Hữu trí tuệ về Quyền tác giả, Quyền liên quan ngày 12 tháng 6 năm 2026 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-draft-decree-implementation-intellectual-property-law-copyright-related-rights.

Khuyến nghị: Luật An ninh dữ liệu không nên lặp lại các nội dung về quản trị AI đã được quy định trong Luật Trí tuệ nhân tạo, bao gồm nội dung về phân loại mức độ rủi ro, nghĩa vụ liên quan đến nội dung do AI tạo ra và khung trách nhiệm đối với các chủ thể liên quan đến AI. Các yêu cầu chồng chéo giữa nhiều văn bản pháp luật có thể tạo ra sự thiếu chắc chắn về mặt pháp lý, dẫn đến việc thực thi không nhất quán và làm gia tăng gánh nặng tuân thủ trùng lặp đối với các tổ chức chịu sự quản lý của nhiều cơ quan khác nhau. Chính phủ Việt Nam nên tránh tạo ra tình trạng chồng chéo và phân mảnh về mặt pháp lý mà Luật An ninh dữ liệu đang hướng tới khắc phục trong khuôn khổ quản trị dữ liệu.

Nhiều giải pháp liên quan đến AI được đề cập trong Hồ Sơ Chính Sách cũng làm phát sinh các quan ngại vượt ra ngoài vấn đề chồng chéo tiềm ẩn với Luật Trí tuệ nhân tạo. Các giải pháp này bao gồm công bố tiêu chuẩn thuật toán, yêu cầu cho phép cơ quan nhà nước tiếp cận mã nguồn hoặc logic vận hành của thuật toán, lưu trữ bắt buộc của nhật ký tạo nội dung và yêu cầu thực hiện thử nghiệm xâm nhập đối với các hệ thống AI lớn nhằm đánh giá các rủi ro về thông tin sai lệch hoặc thao túng dư luận. Mặc dù BSA ủng hộ nỗ lực nhằm ngăn ngừa và xử lý các hành vi sử dụng AI gây hại, những giải pháp nêu trên có thể làm phát sinh các rủi ro đáng kể đối với việc bảo vệ thông tin mật trong kinh doanh, quyền sở hữu trí tuệ, an ninh mạng và hoạt động đổi mới sáng tạo. Ngoài ra, các quan ngại liên quan đến thông tin sai lệch, kiểm duyệt nội dung và thao túng dư luận thường phát sinh trong bối cảnh các nền tảng hướng đến người tiêu dùng như mạng xã hội, công cụ tìm kiếm và các nền tảng giữa doanh nghiệp với người tiêu dùng (**B2C**) khác, thay vì các hệ thống AI của doanh nghiệp và các ứng dụng giữa doanh nghiệp với doanh nghiệp (**B2B**) được thiết kế phục vụ mục đích sử dụng nội bộ của tổ chức.

Khuyến nghị: Luật An ninh dữ liệu nên tránh đặt ra các yêu cầu phải công khai mã nguồn, thuật toán độc quyền, trọng số mô hình (model weights) hoặc các thông tin kỹ thuật mang tính bảo mật và độc quyền khác. Mọi yêu cầu về minh bạch, trách nhiệm giải trình hoặc quản lý rủi ro cần được thiết kế tương xứng với mức độ rủi ro phát sinh và tập trung vào các nhóm hệ thống AI có khả năng cao gây ra các rủi ro đó. Các nghĩa vụ nhằm giải quyết các vấn đề liên quan đến thông tin sai lệch, kiểm duyệt nội dung và thao túng dư luận nên được tập trung áp dụng đối với các nền tảng và dịch vụ hướng tới người tiêu dùng, thay vì các hệ thống AI doanh nghiệp và các ứng dụng doanh nghiệp với doanh nghiệp (B2B). Cách tiếp cận có mục tiêu và dựa trên mức độ rủi ro sẽ giúp giải quyết hiệu quả các quan ngại chính sách công chính đáng, đồng thời duy trì động lực đổi mới sáng tạo, bảo đảm an ninh mạng, bảo vệ quyền sở hữu trí tuệ và khuyến khích đầu tư.

Giai Đoạn Chuyển Tiếp

Luật An ninh dữ liệu giao thẩm quyền đáng kể cho các văn bản hướng dẫn thi hành và Đơn vị Quản trị An ninh Dữ liệu, do đó, phạm vi thực tế của các nghĩa vụ theo luật này — bao gồm cả các tiêu chuẩn kỹ thuật bắt buộc — chỉ thực sự được xác định thông qua các văn bản hướng dẫn và quyết định thực thi sau này. Theo đó, nguyên tắc tham vấn các bên liên quan và nguyên tắc bảo đảm các yêu cầu quản lý phải tương xứng nên được ghi nhận trong luật, thay vì để lại cho cơ quan thực thi toàn quyền quyết định. Việc áp đặt các nghĩa vụ quá sớm, đặc biệt trong trường hợp các tiêu chuẩn kỹ thuật vẫn chưa được xác định rõ, có thể dẫn đến sự thiếu chắc chắn trong tuân thủ mà không mang lại lợi ích tương ứng về an ninh, an toàn dữ liệu.

Khuyến nghị: Luật An ninh dữ liệu cần luật hoá nguyên tắc tham vấn và nguyên tắc tương xứng, đồng thời thiết lập cơ chế tham vấn bắt buộc trước khi ban hành hoặc sửa đổi các quy chuẩn kỹ thuật bắt buộc, theo đó cơ quan có thẩm quyền phải tham vấn các bên liên quan trong ngành. Luật cũng cần quy định các điều khoản chuyển tiếp đối với các kiến trúc hệ thống và các thỏa thuận hợp đồng hiện có đã được xây dựng phù hợp với các quy định pháp luật có hiệu lực tại thời điểm Luật An ninh dữ liệu được ban hành. Bên cạnh đó, các nghĩa vụ tuân thủ nên được triển khai theo lộ trình, với thời gian chuyển tiếp tối thiểu từ 12 đến 18 tháng kể từ ngày các văn bản hướng dẫn được công bố. Điều này sẽ tạo điều kiện để các tổ chức có đủ thời gian chuẩn bị, phân bổ nguồn lực và xây dựng các cơ chế quản trị phù hợp, đáp ứng đồng thời các yêu cầu của pháp luật trong nước và các thông lệ tốt nhất trên phạm vi quốc tế.

Tài Liệu Tham Khảo của BSA

Nhằm hỗ trợ Bộ Công an trong quá trình soạn thảo Luật An ninh dữ liệu, chúng tôi xin gửi kèm các tài liệu liên quan thể hiện quan điểm của BSA, có thể được sử dụng làm nguồn tham khảo hữu ích.

- **Keeping the Door Open: The EU's Path to Digital Sovereignty** (tiếng Việt: Giữ Cánh Cửa Mở: Con Đường Hướng Tới Chủ Quyền Số của Liên minh Châu Âu) trình bày các khuyến nghị của BSA về một cách tiếp cận thực tiễn và cởi mở đối với chủ quyền số tại châu Âu,

- **Enterprise AI Adoption Agenda for ASEAN** (tiếng Việt: Chương Trình Thúc Đẩy Ứng Dụng AI Trong Doanh Nghiệp tại ASEAN) đưa ra các khuyến nghị chính sách dành cho các quốc gia thành viên ASEAN nhằm thúc đẩy việc ứng dụng AI trong doanh nghiệp trên quy mô rộng,

- **Principles for Government Cloud Security Laws and Policies** (tiếng Việt: Các Nguyên Tắc Xây Dựng Pháp Luật và Chính Sách về An Ninh Điện Toán Đám Mây cho Khu Vực Công) trình bày các cách tiếp cận được khuyến nghị trong quá trình xây dựng pháp luật và chính sách về an ninh điện toán đám mây,

- **Quantum Computing and Encryption: Six Actions Governments Should Take to Secure Information** (tiếng Việt: Điện Toán Lượng Tử và Mật Mã: Sáu Hành Động Chính Phủ Cần Thực Hiện để Bảo Vệ Thông Tin) đề xuất các bước cần thiết để các chính phủ chuyển đổi sang các giải pháp mật mã an toàn trước các mối đe dọa từ điện toán lượng tử, và

- **BSA 2026 Quantum Technologies Agenda** (tiếng Việt: Chương Trình Nghị Sự về Công Nghệ Lượng Tử của BSA năm 2026) đưa ra các khuyến nghị dành cho chính phủ nhằm xây dựng và duy trì vai trò dẫn dắt trong lĩnh vực công nghệ lượng tử trong dài hạn.

Kết luận

Chúng tôi xin cảm ơn Bộ Công an đã xem xét các ý kiến đóng góp của chúng tôi đối với Luật An ninh dữ liệu và hy vọng Quý cơ quan sẽ tích cực cân nhắc các khuyến nghị của chúng tôi. Chúng tôi trân trọng đề nghị Bộ Công an tiếp tục duy trì đối thoại với khu vực tư nhân và thúc đẩy các thảo luận cởi mở nhằm hướng tới mục tiêu chung là xây dựng một nền kinh tế số năng động và có năng lực cạnh tranh cao. Nếu Quý Bộ cần thêm thông tin hoặc làm rõ bất kỳ nội dung nào, xin vui lòng liên hệ với chúng tôi. Một lần nữa, chúng tôi xin trân trọng cảm ơn Quý Bộ đã dành thời gian và quan tâm xem xét các ý kiến đóng góp này.

Trân trọng,

Wong Wai San
Giám đốc, Chính sách – Châu Á-Thái Bình Dương