Ngày 06 tháng 3 năm 2026

BSA GÓP Ý DỰ THẢO NGHỊ ĐỊNH QUY ĐỊNH CHI TIẾT MỘT SỐ ĐIỀU CỦA LUẬT AN NINH MẠNG

Kính gửi: **- Bộ Công an**

- Bộ Tư pháp

Thay mặt Liên minh Phần mềm (**BSA**),[1] bằng thư này, tôi xin gửi tới Quý Cơ quan các khuyến nghị chính sách của chúng tôi liên quan đến quá trình soạn thảo, thẩm định và rà soát dự thảo Nghị định quy định chi tiết một số điều của Luật An ninh mạng đề ngày 24 tháng 2 năm 2026 (**Dự Thảo Nghị Định**). BSA là hiệp hội thương mại toàn cầu của ngành công nghiệp phần mềm. Các thành viên của chúng tôi là những doanh nghiệp đi 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 phối hợp với Bộ Công an về các vấn đề an ninh mạng[2] và gần đây nhất chúng tôi cũng đã gửi ý kiến đóng góp đối với Luật An ninh mạng.[3]

Thời gian lấy ý kiến công khai không đủ

Thời gian lấy ý kiến góp ý đối với Dự Thảo Nghị Định được bắt đầu từ ngày 13 tháng 02 và kết thúc vào ngày 22 tháng 02 năm 2026, trùng với kỳ nghỉ Tết Nguyên đán. Mặc dù việc Chính phủ tổ chức lấy ý kiến công khai là đáng ghi nhận, nhưng thời gian lấy ý kiến ngắn – đặc biệt là khi khoảng thời gian này lại trùng với một kỳ nghỉ lễ lớn của cả nước – đã khiến cho các bên liên quan không có đủ thời gian để đưa ra các ý kiến đóng góp một cách toàn diện và có chất lượng. Việc gia hạn thời gian lấy ý kiến đối với Dự Thảo Nghị Định là rất quan trọng nhằm bảo đảm sự tham gia đầy đủ của các bên liên quan và giúp quá trình soạn thảo Dự Thảo Nghị Định được xem xét một cách thấu đáo. Việc tiến hành lấy ý kiến trong một khoảng thời gian gấp rút có thể khiến cơ quan soạn thảo bỏ sót những ý kiến đóng góp quan trọng, dẫn đến các hệ quả ngoài ý muốn, chẳng hạn như những khoảng trống trong quy định hoặc các yêu cầu tuân thủ quá mức cần thiết.

---

[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 và Zoom Communications Inc.

[2] Ví dụ bao gồm việc tham dự Hội thảo về 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, Ý kiến đóng góp về Nghị định 53 vào tháng 9 năm 2022, xem tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-decree-53-to-implement-the-law-on-cybersecurity; và các ý kiến đề xuất sửa đổi dự thảo Nghị định 72 vào tháng 9 và tháng 12 năm 2021, xem tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposed-amendments-to-draft-decree-72-0.

[3] Góp ý của BSA về Dự thảo Luật An ninh mạng ngày 8 tháng 8 năm 2025, và ngày 26 tháng 9 năm 2025 xem tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-cybersecurity-law-dated-8-august-2025.

Chúng tôi trân trọng đề nghị các ý kiến của mình được xem xét trong quá trình các Quý Cơ quan rà soát và thẩm định Dự Thảo Nghị Định, và đề nghị Bộ Công an xem xét gia hạn thời gian lấy ý kiến đối với Dự Thảo Nghị Định nhằm đảm bảo các ý kiến đóng góp được đưa ra một cách toàn diện và có chất lượng, cũng như đảm bảo cơ hội tham gia đóng góp ý kiến của tất cả các đối tượng chịu sự ảnh hưởng.

Do thời gian hạn chế để nghiên cứu bản dự thảo mới nhất đề ngày 24 tháng 2 năm 2026, chúng tôi tập trung góp ý vào hai nhóm vấn đề ưu tiên: báo cáo sự cố và yêu cầu lưu trữ dữ liệu tại Việt Nam. Việc chúng tôi tập trung đóng góp ý kiến đối với hai nhóm vấn đề này không nên được hiểu rằng BSA không có quan ngại đối với các quy định khác của Dự Thảo Nghị Định. Thay vào đó, chúng tôi muốn nhấn mạnh các vấn đề mang tính cấp thiết cao và sẵn sàng tiếp tục đóng góp ý kiến khi có thêm thông tin.

Định nghĩa

Luật An ninh mạng đưa ra các thuật ngữ có nội hàm rộng, ví dụ như "*sự cố an ninh mạng*", "*dịch vụ an ninh mạng*" và các nhà cung cấp dịch vụ an ninh mạng. Dự Thảo Nghị Định không đưa ra thêm giải thích về định nghĩa của các thuật ngữ này. Hơn nữa, dự thảo còn đề cập đến các thuật ngữ mới như "*dữ liệu cốt lõi*", "*dữ liệu quan trọng*" và "*cơ quan có thẩm quyền*" mà không có định nghĩa cụ thể. Việc thiếu các định nghĩa rõ ràng đối với các thuật ngữ này làm tăng nguy cơ diễn giải và thực thi không nhất quán.

Khuyến nghị: Các định nghĩa và bất kỳ nghĩa vụ nào được quy định cần phải rõ ràng, hiệu quả, khả thi và tương xứng với rủi ro thực tế liên quan. Ví dụ, một sự cố an ninh mạng cần báo cáo nên được định nghĩa hẹp hơn để chỉ bao gồm các sự cố mạng thực tế, nghiêm trọng và làm ảnh hưởng đến khả năng thực hiện các chức năng quan trọng của doanh nghiệp, thay vì bao gồm cả các hoạt động bị nghi ngờ hoặc những hoạt động chỉ gây rủi ro, đe dọa hoặc làm tăng khả năng xảy ra sự cố mạng. Nếu "*dữ liệu cốt lõi*" và "*dữ liệu quan trọng*" sẽ có cùng định nghĩa như trong Luật Dữ liệu, điều này cần được nêu rõ để đảm bảo tính nhất quán trong toàn bộ khung pháp lý. Dự Thảo Nghị Định cũng cần quy định rõ ràng những cơ quan nào đủ điều kiện là "*cơ quan có thẩm quyền*" để báo cáo sự cố.

Yêu cầu báo cáo sự cố

Khoản 1 Điều 36 Dự Thảo Nghị Định quy định "*khi xảy ra sự cố lộ, mất dữ liệu cốt lõi hoặc dữ liệu quan trọng, chủ quản hệ thống thông tin có trách nhiệm: a) Kích hoạt ngay phương án ứng phó sự cố đã được phê duyệt; b) Thông báo cho cơ quan có thẩm quyền trong thời hạn 24 giờ kể từ khi phát hiện sự cố; trường hợp sự cố nghiêm trọng đe dọa an ninh quốc gia thì phải thông báo ngay nhưng không quá 03 giờ.*" Ngoài ra, Dự Thảo Nghị Định cũng không định nghĩa như thế nào là một "*sự cố lộ, mất*" "*dữ liệu cốt lõi*" hoặc "*dữ liệu quan trọng*", hay đưa ra một ngưỡng cụ thể mà chỉ khi vượt ngưỡng đó sự cố sẽ phải được báo cáo.

Khoảng thời gian quá ngắn không cho phép các tổ chức có đủ thời gian để điều tra sự cố, đánh giá liệu đây có phải là sự cố thuộc diện phải báo cáo hay không, và liệu đây có phải là một sự cố nghiêm trọng đe dọa an ninh quốc gia. Quy định hiện tại yêu cầu thông báo cho cơ quan có thẩm quyền trong vòng 24 giờ, và trong vòng 3 giờ đối với sự cố nghiêm trọng đe dọa an ninh quốc gia, là

không khả thi, không thực tế và cũng không phù hợp với thông lệ quốc tế. Các tổ chức cần có đủ thời gian để điều tra sự cố, đánh giá mức độ ảnh hưởng và triển khai biện pháp khắc phục nhằm giảm thiểu thiệt hại trước khi thực hiện báo cáo.

Khuyến nghị: Như đã nêu trong ý kiến góp ý trước đây của chúng tôi,[4] BSA khuyến nghị Chính phủ Việt Nam điều chỉnh và hài hòa các nghĩa vụ báo cáo sự cố mạng với thông lệ quốc tế tốt nhất, bao gồm việc xác định thế nào là sự cố mạng, thời hạn và ngưỡng yêu cầu thông báo và loại thông tin cần phải cung cấp cho cơ quan chức năng. Như được nêu trong *10 Nguyên Tắc Của BSA Về Hài Hòa Hóa Báo Cáo Sự Cố Mạng Trên Toàn Cầu*,[5] việc các yêu cầu được hài hòa giúp tạo nên một bộ dữ liệu thống nhất, từ đó các bên liên quan có thể chia sẻ thông tin một cách hiệu quả, tăng cường hiểu biết về các mối đe dọa, cải thiện quản lý lỗ hổng, điều chỉnh các biện pháp kiểm soát an ninh, và đẩy nhanh ứng phó sự cố. Dự Thảo Nghị Định nên quy định thời hạn báo cáo sự cố phù hợp với thông lệ quốc tế và tương ứng với mức độ thông tin cần phải cung cấp, ví dụ: Chỉ Thị An Ninh Mạng Và Thông Tin Của EU (**NIS2**) quy định thời hạn 24 giờ để thông báo[6] và Đạo Luật Báo Cáo Sự Cố Mạng Đối Với Cơ Sở Hạ Tầng Quan Trọng Của Hoa Kỳ (**CIRCIA**) cho phép tối thiểu 72 giờ để nộp báo cáo.[7]

Yêu cầu lưu trữ dữ liệu tại Việt Nam

Điều 28 yêu cầu doanh nghiệp trong nước lưu trữ một số loại dữ liệu tại Việt Nam: a) Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam; b) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra: Tên tài khoản sử dụng dịch vụ, thời gian sử dụng dịch vụ, thông tin thẻ tín dụng, địa chỉ thư điện tử, địa chỉ mạng (IP) đăng nhập, đăng xuất gần nhất, số điện thoại đăng ký được gắn với tài khoản hoặc dữ liệu; c) Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác. Ngoài ra, Khoản 3 Điều 28 yêu cầu các doanh nghiệp nước ngoài – bao gồm các doanh nghiệp cung cấp dịch vụ lưu trữ và chia sẻ dữ liệu trên không gian mạng, ứng dụng trực tuyến và các dịch vụ tương tự – phải thành lập chi nhánh hoặc văn phòng đại diện tại Việt Nam trong một số trường hợp cụ thể liên quan đến việc vi phạm quy định của Luật An ninh mạng và đã được Bộ Công an thông báo.

Theo cách hiểu của BSA, các yêu cầu nêu tại Điều 28 của Dự Thảo Nghị Định tương tự như các quy định về yêu cầu lưu trữ dữ liệu tại Việt Nam nêu tại Nghị Định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 quy định chi tiết một số điều của Luật An ninh mạng 2018 (**Nghị định 53**).

Phạm vi dịch vụ được đề xuất cho việc lưu trữ dữ liệu tại Việt Nam rất rộng và có khả năng bao gồm các doanh nghiệp, kể cả những doanh nghiệp thường hoạt động với tư cách là bên xử lý dữ liệu, tức là các nhà cung cấp dịch vụ xử lý thông tin cá nhân thay mặt cho một bên khác (tức là bên kiểm soát dữ liệu). Cả hai bên này đều có vai trò và trách nhiệm riêng biệt liên quan đến hoạt

[4] Góp ý của BSA về Dự thảo Luật An ninh mạng ngày 8 tháng 8 năm 2025, và ngày 26 tháng 9 năm 2025 xem tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-cybersecurity-law-dated-8-august-2025.

[5] 10 Nguyên Tắc Của BSA Về Hài Hòa Hóa Báo Cáo Sự Cố Mạng Trên Toàn Cầu, tháng 2 năm 2025, xem tại https://www.bsa.org/policy-filings/global-10-principles-for-cyber-incident-reporting-harmonization-around-the-globe .

[6] Chỉ thị (EU) 2022/2555 của Nghị viện Châu Âu và của Hội đồng ngày 14 tháng 12 năm 2022 về các biện pháp nhằm đạt được mức độ an ninh mạng chung cao trên toàn Liên minh ngày 27 tháng 12 năm 2022, xem tại https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[7] Đạo Luật Báo Cáo Sự Cố Mạng Đối Với Cơ Sở Hạ Tầng Quan Trọng năm 2022, tháng 3 năm 2022, xem tại https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

động xử lý dữ liệu, đã được phân biệt rõ ràng theo Luật Bảo vệ Dữ liệu Cá nhân (Luật BVDLCN) của Việt Nam có hiệu lực từ tháng 1 năm 2026. Luật BVDLCN giao cho bên kiểm soát dữ liệu trách nhiệm chính đối với các hoạt động xử lý dữ liệu vì bên xử lý dữ liệu chỉ hoạt động dựa trên hướng dẫn và chỉ thị của bên kiểm soát dữ liệu.

Nếu cả bên kiểm soát dữ liệu và bên xử lý dữ liệu đều phải tuân thủ các tiêu chuẩn lưu trữ dữ liệu tại Việt Nam được quy định nghiêm ngặt, điều này sẽ gia tăng thêm chi phí cho nền kinh tế số, dưới hình thức yêu cầu lưu trữ bổ sung, phát sinh các vấn đề về an ninh thông tin, sự không chắc chắn về quy định, cũng như gánh nặng tuân thủ chồng chéo.

Việc chuyển dữ liệu xuyên biên giới là nền tảng của nền kinh tế toàn cầu và đóng vai trò thiết yếu đối với an ninh mạng và an toàn hệ thống thông tin. Các yêu cầu lưu trữ dữ liệu tại Việt Nam không giúp gia tăng việc đảm bảo an toàn thông tin, thậm chí có thể gây tác dụng ngược bằng cách làm suy giảm mức độ an ninh thông tin. Những yêu cầu như vậy có thể cản trở nỗ lực triển khai các biện pháp an ninh hiệu quả, nỗ lực bảo vệ dữ liệu và bảo vệ các mạng lưới trọng yếu, đồng thời hạn chế đổi mới sáng tạo trong kinh doanh và hạn chế các dịch vụ có thể cung cấp cho người tiêu dùng.

Như đã nêu trong các kiến nghị trước đây, yêu cầu lưu trữ dữ liệu tại Việt Nam có thể gây tác động tiêu cực tới nền kinh tế trong nước, khi chúng hạn chế khả năng của các doanh nghiệp và tổ chức trong nước trong việc áp dụng đầy đủ các công nghệ và dịch vụ tiên tiến hiện có trên thị trường toàn cầu. Ví dụ, các hạn chế đối với việc chuyển dữ liệu xuyên biên giới có thể khiến doanh nghiệp Việt Nam, bao gồm cả doanh nghiệp vừa và nhỏ (**SME**) lẫn các tổ chức lớn như bệnh viện, hãng hàng không hay ngân hàng, không thể sử dụng các giải pháp công nghệ thông tin và điện toán đám mây hàng đầu thế giới do các nhà cung cấp dịch vụ nước ngoài cung cấp. Các dịch vụ này thường mang lại năng lực bảo vệ vượt trội. Những doanh nghiệp trong nước phải tuân thủ hạn chế chuyển dữ liệu nhiều khả năng sẽ gặp khó khăn trong việc tiếp cận các dịch vụ này, làm giảm khả năng cạnh tranh, đặc biệt trên thị trường quốc tế, đồng thời khiến họ phải đối mặt với rủi ro bảo vệ dữ liệu lớn hơn. Các hạn chế đối với chuyển dữ liệu quốc tế cũng tạo ra gánh nặng đáng kể trong việc quản lý đối với các cơ quan nhà nước.

Hơn nữa, việc yêu cầu lưu trữ tại Việt Nam đối với các nhóm dữ liệu rộng, có thể bao gồm cả những loại dữ liệu phổ biến trong hoạt động kinh doanh hàng ngày, là không phù hợp. Những loại dữ liệu này khác với dữ liệu nhạy cảm của cơ quan nhà nước có liên quan đến các vấn đề an ninh quốc gia. Do đó, chúng tôi đề nghị Việt Nam tránh áp đặt các hạn chế không cần thiết hoặc tùy tiện đối với hoạt động chuyển dữ liệu xuyên biên giới, đặc biệt khi Việt Nam đang có mức độ hạn chế tương đối cao theo các chỉ số quốc tế về chính sách chuyển dữ liệu xuyên biên giới.[8] Nỗ lực xây dựng khung pháp lý của Việt Nam nên tập trung vào việc tạo điều kiện thuận lợi cho hoạt động chuyển dữ liệu xuyên biên giới trong nền kinh tế số – phù hợp với các cam kết quốc tế của Việt Nam, chẳng hạn như theo Điều 12 của Thỏa thuận Thương mại Điện tử thuộc WTO về việc "*tạo điều kiện cho công chúng truy cập và sử dụng dữ liệu của Chính phủ*" và Điều 14.11 của Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (**CPTPP**) – đồng thời xem xét một cách tiếp

[8] Liên Minh Dữ Liệu Toàn Cầu, *Chỉ số Chính sách Dữ liệu Xuyên biên giới* (2023), xem tại: https://globaldataalliance.org/resource/cross-border-data-policy-index/

cận phù hợp hơn đối với quản trị dữ liệu, không ảnh hưởng đến mục tiêu an ninh quốc gia và chính sách công.[9]

Khuyến nghị: Loại bỏ yêu cầu lưu trữ dữ liệu tại Việt Nam quy định tại Điều 28 mà buộc các tổ chức thuộc phạm vi điều chỉnh phải lưu trữ dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ và dữ liệu do người sử dụng dịch vụ tạo ra tại Việt Nam. Nếu Bộ Công an muốn giữ lại các yêu cầu lưu trữ dữ liệu tại Việt Nam, ngược lại với khuyến nghị của chúng tôi, chúng tôi xin khuyến nghị Bộ Công an làm rõ rằng miễn là dữ liệu được lưu trữ tại Việt Nam, yêu cầu được đề xuất tại Điều 28 sẽ không (a) hạn chế doanh nghiệp chuyển một bản sao của dữ liệu ra nước ngoài cho mục đích kinh doanh hợp pháp, và đồng thời không (b) cản trở doanh nghiệp sử dụng các dịch vụ điện toán đám mây toàn cầu mà không hoặc không thể lưu trữ dữ liệu tại Việt Nam.

Kết luận

Chúng tôi xin cảm ơn Bộ Công an và Bộ Tư pháp đã xem xét các ý kiến của chúng tôi đối với Dự Thảo Nghị Định và chúng tôi hy vọng rằng Chính phủ Việt Nam sẽ cân nhắc một cách tích cực các khuyến nghị của chúng tôi. Chúng tôi hy vọng Bộ Công an và Bộ Tư pháp sẽ tiếp tục đối thoại với khu vực tư nhân và duy trì các cuộc trao đổi cởi mở nhằm đạt được các mục tiêu chung trong việc xây dựng một nền kinh tế số năng động và cạnh tranh. Xin vui lòng liên hệ với chúng tôi nếu Quý Cơ quan cần làm rõ hoặc cung cấp thêm thông tin. Một lần nữa, xin trân trọng cảm ơn Quý Bộ đã dành thời gian xem xét.

Trân trọng,

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

[9] Dữ liệu mở - Thu hẹp khoảng cách dữ liệu (2021), xem tại https://www.bsa.org/files/policy-filings/061120bsaopendata.pdf