Ngày 9 tháng 11 năm 2026

Thượng tướng Lê Tấn Tới
Chủ nhiệm
Ủy ban Quốc phòng, An ninh và Đối ngoại
Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam
Hà Nội, Việt Nam

V/v: ***Góp ý của Association for Competitive Technology (ACT) gửi Ủy ban Quốc phòng, An ninh và Đối ngoại của Quốc hội Việt Nam về dự thảo Luật An ninh dữ liệu***

Kính gửi Thượng tướng Lê Tấn Tới, Chủ nhiệm Ủy ban,

Association for Competitive Technology (ACT – Hiệp hội Công nghệ Cạnh tranh) trân trọng cảm ơn cơ hội được chia sẻ ý kiến về dự thảo Luật An ninh dữ liệu đã được chỉnh lý (sau đây gọi là "dự thảo Luật"), được Chính phủ trình Quốc hội ngày 26 tháng 10 năm 2026 và được Ủy ban đánh giá là đủ điều kiện trình Quốc hội xem xét, thông qua tại Kỳ họp này.[1]

I. Giới thiệu và mối quan tâm của ACT

ACT là hiệp hội thương mại phi lợi nhuận đại diện cho cộng đồng các nhà phát triển công nghệ là doanh nghiệp nhỏ trên toàn cầu. Các thành viên của chúng tôi xây dựng phần mềm, ứng dụng di động, thiết bị kết nối và dịch vụ dựa trên điện toán đám mây, bao gồm các nhà phát triển có trụ sở tại Việt Nam và các công ty trên khắp thế giới phục vụ người tiêu dùng và doanh nghiệp Việt Nam. Các nhà phát triển nhỏ phụ thuộc vào dịch vụ điện toán đám mây an toàn với chi phí hợp lý, mã hóa mạnh và khả năng chuyển dữ liệu xuyên biên giới để tiếp cận khách hàng và cạnh tranh với các doanh nghiệp lớn hơn.

ACT ủng hộ mục tiêu của Việt Nam trong việc bảo vệ dữ liệu có liên quan đến an ninh quốc gia, trật tự, an toàn xã hội và ghi nhận những tiến bộ thực chất trong dự thảo đã được chỉnh lý. Chúng tôi đánh giá cao việc Ủy ban ủng hộ cách tiếp cận đối với dữ liệu xuyên biên giới tập trung vào các biện pháp kiểm soát an ninh thay vì yêu cầu lưu trữ dữ liệu tại Việt Nam. Các ý kiến của chúng tôi nhằm giúp dự thảo Luật đạt được các mục tiêu an ninh mà không đặt ra cho các nhà phát triển nhỏ những nghĩa vụ mà họ không thể đáp ứng hoặc khiến họ bị tách khỏi các dịch vụ và khách hàng mà họ phụ thuộc. Chúng tôi mong các ý kiến này được xem xét khi hoàn thiện văn bản cuối cùng và, sau khi Luật được thông qua, khi xây dựng các nghị định hướng dẫn thi hành.

II. Sự thống nhất với các luật hiện hành của Việt Nam về dữ liệu

[1] Đại tướng Lương Tam Quang, Bộ trưởng Bộ Công an, đã trình bày Tờ trình của Chính phủ và Ủy ban đã trình bày Báo cáo thẩm tra tại phiên họp toàn thể của Quốc hội ngày 26 tháng 10 năm 2026. Xem "Hoàn thiện hệ thống pháp luật, tạo điều kiện phát triển kinh tế dữ liệu," Tạp chí Thị trường Tài chính Tiền tệ (26/10/2026), https://thitruongtaichinhtiente.vn/hoan-thien-he-thong-phap-luat-tao-dieu-kien-phat-trien-kinh-te-du-lieu-86576.html.

Các nhà phát triển nhỏ hiếm khi có nhân sự chuyên trách về tuân thủ. Vì vậy, khi dữ liệu cùng chịu sự điều chỉnh của Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, Luật An ninh mạng, Luật Trí tuệ nhân tạo và dự thảo Luật, mỗi luật có hệ thống phân loại, ngưỡng áp dụng và chu kỳ báo cáo riêng, thì chi phí tuân thủ đè nặng nhất lên các doanh nghiệp nhỏ nhất. Chúng tôi đề nghị Ủy ban bảo đảm rằng các cấp độ phân loại trong dự thảo Luật tương ứng với các loại dữ liệu trong Luật Dữ liệu; rằng một báo cáo đánh giá tác động có thể đáp ứng yêu cầu của từng luật khi cùng một tập dữ liệu chịu sự điều chỉnh của nhiều luật; rằng báo cáo đánh giá được lập một lần và cập nhật khi có thay đổi đáng kể, như quy định tại Nghị định 165 và Nghị định 356, thay vì phải nộp lại hằng năm; và rằng doanh nghiệp không phải chịu các nghĩa vụ lưu trữ hoặc lưu giữ riêng rẽ đối với cùng một dữ liệu theo các luật khác nhau.

Dự thảo Luật cũng nên tuân theo cách phân định vai trò đã được quy định trong Luật Bảo vệ dữ liệu cá nhân và Luật Dữ liệu. Các nghĩa vụ đòi hỏi phải biết dữ liệu là gì và được xử lý nhằm mục đích gì, như phân loại, đánh giá rủi ro và quyết định chuyển dữ liệu, nên thuộc về bên kiểm soát dữ liệu. Nhà cung cấp dịch vụ đám mây hoặc phần mềm đóng vai trò bên xử lý dữ liệu, vốn thường không nắm được nội dung dữ liệu của khách hàng, nên chịu trách nhiệm về các biện pháp bảo đảm an ninh nằm trong phạm vi kiểm soát thực tế của mình.

III. Phân loại dữ liệu dựa trên rủi ro

Chúng tôi đề nghị các cấp độ rủi ro cao hơn, đặc biệt là cấp độ 4 và cấp độ 5, được xác định theo các tiêu chí khách quan quy định trong Luật hoặc trong nghị định được ban hành sau khi lấy ý kiến công khai. Các cấp độ này chỉ nên áp dụng đối với dữ liệu mà nếu bị xâm phạm sẽ ảnh hưởng trực tiếp đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc hoạt động của hạ tầng trọng yếu quốc gia. Dữ liệu không nên bị xếp vào cấp độ cao hơn chỉ vì được một doanh nghiệp trong một lĩnh vực nhất định, như tài chính, y tế hoặc viễn thông, nắm giữ, hoặc vì tập dữ liệu đã đạt đến một quy mô nhất định. Hồ sơ khách hàng của một ứng dụng y tế nhỏ hay một công ty khởi nghiệp về thanh toán không nên phải chịu các nghĩa vụ dành cho dữ liệu có liên quan trực tiếp đến an ninh quốc gia. Các tiêu chí được công bố công khai sẽ tạo cơ sở thống nhất cho các cơ quan thi hành Luật khi ra quyết định, đồng thời mang lại cho doanh nghiệp sự chắc chắn cần thiết để đầu tư.

IV. Chuyển dữ liệu xuyên biên giới

Chúng tôi chia sẻ quan điểm của Phó Chủ tịch Quốc hội Nguyễn Hồng Diên rằng quy định về chuyển dữ liệu xuyên biên giới cần tính đến rủi ro của từng hoạt động chuyển dữ liệu cụ thể, bên cạnh cấp độ phân loại của dữ liệu.[2] Mục đích chuyển dữ liệu, bên nhận, phạm vi xử lý, biện pháp mã hóa được áp dụng và khả năng thu hồi dữ liệu đều ảnh hưởng đến mức độ rủi ro đó. Việc chuyển dữ liệu đã được mã hóa để xử lý kỹ thuật, với quyền truy cập bị hạn chế và có khả năng thu hồi, có mức độ rủi ro rất khác so với việc chuyển dữ liệu chưa được mã hóa ra nước ngoài để lưu trữ lâu dài. Các hoạt động thường xuyên như xử lý thanh toán, lưu trữ trên nền tảng điện toán đám mây, cập nhật phần mềm, hỗ trợ khách hàng và vận hành các hệ thống tập trung nên được thực hiện chỉ trên cơ sở đánh giá nội bộ và lưu giữ hồ sơ. Do đó, chúng tôi đề nghị Ủy ban:

[2] Phát biểu của Phó Chủ tịch Quốc hội Nguyễn Hồng Diên tại Phiên họp thứ 6 của Ủy ban Thường vụ Quốc hội. Xem "Thiết lập khung pháp lý bảo vệ tài nguyên dữ liệu quốc gia từ sớm, từ xa," Đại biểu Nhân dân (27/9/2026), https://daibieunhandan.vn/thiet-lap-khung-phap-ly-bao-ve-tai-nguyen-du-lieu-quoc-gia-tu-som-tu-xa-10431931.html.

1. Chỉ áp dụng thủ tục đánh giá và chấp thuận trước đối với việc chuyển dữ liệu cấp độ 4 và cấp độ 5 được xác định trong phạm vi hẹp, với thời hạn xem xét cố định và quyết định bằng văn bản nêu rõ lý do.
2. Không cấm tuyệt đối việc chuyển dữ liệu do khu vực tư nhân nắm giữ. Nếu vẫn duy trì quy định cấm đối với một nhóm hẹp dữ liệu quốc phòng, an ninh do Nhà nước nắm giữ, Luật cần quy định rõ tiêu chí, trình tự và thời hạn cho phép các trường hợp ngoại lệ.
3. Công nhận các cơ chế chuyển dữ liệu được quốc tế chấp nhận, bao gồm Điều khoản hợp đồng mẫu ASEAN, Hệ thống Quy tắc bảo vệ quyền riêng tư xuyên biên giới toàn cầu (Global CBPR), Điều khoản hợp đồng tiêu chuẩn của EU và chứng nhận ISO/IEC 27001, là căn cứ hợp lệ để chuyển dữ liệu mà không phải thực hiện thêm thủ tục chấp thuận hoặc báo cáo.
4. Bãi bỏ mọi yêu cầu còn lại về lưu trữ tại Việt Nam đối với dữ liệu do khu vực tư nhân nắm giữ, để Luật tập trung vào kết quả bảo đảm an ninh. Cách tiếp cận này cũng phù hợp với các cam kết của Việt Nam về luồng dữ liệu xuyên biên giới và vị trí đặt cơ sở điện toán.[3]

V. **Khóa giải mã và mã hóa**

Theo hiểu biết của chúng tôi, dự thảo đã được chỉnh lý sẽ hạn chế việc chuyển ra ngoài lãnh thổ Việt Nam các khóa giải mã và tham số mật mã gắn với dữ liệu cấp độ 4 và cấp độ 5. Mã hóa là một trong những công cụ bảo đảm an ninh hiệu quả nhất mà các nhà phát triển nhỏ có thể sử dụng. Nhiều nhà phát triển dựa vào dịch vụ quản lý khóa của các nhà cung cấp dịch vụ đám mây quốc tế, hoặc vào các giải pháp mã hóa được thiết kế để chỉ người dùng cuối nắm giữ khóa. Để quy định hạn chế đối với khóa không trở thành một yêu cầu lưu trữ dữ liệu theo một cách khác hoặc làm suy giảm mức độ an ninh của các dịch vụ mà người dùng Việt Nam đang sử dụng, chúng tôi đề nghị văn bản cuối cùng:

1. Chỉ áp dụng quy định hạn chế đối với các khóa bảo vệ dữ liệu được phân loại ở cấp độ 4 hoặc cấp độ 5 theo các tiêu chí khách quan.
2. Quy định rõ rằng Luật không yêu cầu bất kỳ nhà cung cấp nào phải tạo lập, nắm giữ, lưu giữ hoặc tiết lộ khóa giải mã mà thông thường họ không nắm giữ, hoặc phải thiết kế lại cơ chế mã hóa đầu cuối hoặc mã hóa trên thiết bị trong đó khóa do người dùng nắm giữ.
3. Cho phép tổ chức đáp ứng yêu cầu thông qua các cơ chế quản lý khóa do chính tổ chức kiểm soát, bao gồm khóa do khách hàng quản lý và mô-đun bảo mật phần cứng (HSM) được chứng nhận theo các tiêu chuẩn được quốc tế công nhận, mà không bắt buộc sử dụng một địa điểm hoặc nhà cung cấp cụ thể.
4. Không đặt ra bất kỳ yêu cầu nào về cơ chế cho phép bên thứ ba giải mã dữ liệu mà không có sự tham gia của bên nắm giữ khóa. Bất kỳ cơ chế nào như vậy đều tạo ra điểm yếu mà tội phạm và các chủ thể thù địch cũng có thể khai thác, và sẽ làm giảm mức độ an toàn của dữ liệu Việt Nam. Việt Nam cũng đã cam kết không yêu cầu nhà sản xuất hoặc nhà cung cấp các sản phẩm thương mại có sử dụng mật mã phải chuyển giao hoặc cho phép truy cập khóa riêng như một điều kiện gia nhập thị trường trên thực tế, thông qua việc đặt yêu cầu đó

[3] Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), Điều 14.11 (Chuyển thông tin xuyên biên giới bằng phương tiện điện tử) và Điều 14.13 (Vị trí đặt cơ sở điện toán).

làm điều kiện cho việc sản xuất, bán, phân phối, nhập khẩu hoặc sử dụng các sản phẩm này.[4]

VI. Biện pháp kỹ thuật và bảo đảm trình tự, thủ tục

Chúng tôi hoan nghênh việc Ủy ban ủng hộ giới hạn thời hạn 90 ngày đối với các biện pháp kỹ thuật áp dụng với dịch vụ xuyên biên giới. Đối với một nhà phát triển nhỏ, ngay cả việc bị chặn tạm thời cũng có thể khiến họ mất những khách hàng khó có thể giành lại. Do đó, chúng tôi đề nghị văn bản cuối cùng:

1. Yêu cầu có quyết định bằng văn bản nêu rõ căn cứ đối với bất kỳ biện pháp kỹ thuật nào, kèm theo thông báo và cơ hội khắc phục trước khi biện pháp có hiệu lực, trừ trường hợp thực sự khẩn cấp.
2. Áp dụng biện pháp đối với đúng dịch vụ và chủ thể chịu trách nhiệm về vi phạm, không áp dụng đối với các nền tảng, hạ tầng điện toán đám mây hoặc các nhà phát triển khác có dịch vụ dùng chung hạ tầng đó.
3. Coi 90 ngày là thời hạn tối đa và quy định cơ chế để đề nghị xem xét lại quyết định.

VII. Trí tuệ nhân tạo và thông tin kinh doanh bí mật

Dự thảo tháng 8 có quy định các nghĩa vụ đối với nhà cung cấp dịch vụ trí tuệ nhân tạo liên quan đến dữ liệu huấn luyện, gắn nhãn và giải thích thuật toán. Trong trường hợp văn bản cuối cùng vẫn giữ các quy định này, chúng tôi đề nghị để Luật Trí tuệ nhân tạo và các nghị định hướng dẫn thi hành điều chỉnh các nội dung này, vì các văn bản đó đã quy định về những vấn đề này, nhằm tránh việc nhà phát triển phải tuân thủ hai bộ quy định cho cùng một hoạt động. Mọi yêu cầu của cơ quan có thẩm quyền về cung cấp thông tin liên quan đến thuật toán hoặc hệ thống cần bảo vệ mã nguồn, trọng số mô hình, nguồn dữ liệu huấn luyện và các bí mật kinh doanh khác khỏi bị tiết lộ, bởi đối với nhiều nhà phát triển nhỏ, tài sản trí tuệ này là tài sản có giá trị nhất của họ.

VIII. Triển khai thực hiện tương xứng

Cuối cùng, chúng tôi đề nghị Ủy ban ủng hộ các biện pháp sau để các doanh nghiệp nhỏ có thể tuân thủ trên thực tế:

1. Thống nhất thời hạn và ngưỡng báo cáo sự cố giữa các luật của Việt Nam và phù hợp với thông lệ quốc tế, theo đó thường cho phép 24 giờ để thông báo ban đầu và 72 giờ để báo cáo đầy đủ hơn.
2. Tính các khoản phạt theo tỷ lệ phần trăm trên doanh thu tại Việt Nam của chủ thể vi phạm, không tính trên tổng doanh thu toàn cầu của tập đoàn, và quy định ngay trong Luật các hành vi vi phạm bị áp dụng mức phạt này.
3. Công bố các nghị định hướng dẫn thi hành, kèm theo các mẫu đánh giá đơn giản hóa và tài liệu hướng dẫn dành cho doanh nghiệp nhỏ, để lấy ý kiến công khai trong thời gian ít nhất 60 ngày, và quy định thời gian chuyển tiếp sau khi Luật có hiệu lực vào ngày 1 tháng 7 năm 2027 để doanh nghiệp nhỏ có thời gian điều chỉnh hệ thống và hợp đồng.

[4] CPTPP, Phụ lục 8-B, Mục A (Sản phẩm công nghệ thông tin và truyền thông sử dụng mật mã), đoạn 3.

IX. Kết luận

ACT trân trọng cảm ơn Ủy ban đã xem xét các ý kiến này. Chúng tôi mong có cơ hội làm việc với Ủy ban hoặc Bộ Công an để trao đổi về các ý kiến trên, và đóng góp vào việc xây dựng các tiêu chí khách quan cho cấp độ 4 và cấp độ 5 cũng như các nghị định hướng dẫn thi hành.

Trân trọng,



Brian Scarpelli
Cố vấn Chính sách Toàn cầu Cấp cao

Chapin Gregor
Cố vấn Chính sách Toàn cầu

Association for Competitive Technology
1401 K St NW (Ste 501)
Washington, DC 20005
United States

Đồng gửi: Ông Trần Thanh Mẫn, Chủ tịch Quốc hội
Ông Nguyễn Hồng Diên, Phó Chủ tịch Quốc hội
Đại tướng Lương Tam Quang, Bộ trưởng Bộ Công an